ISSN 2704-8012

European Journal of Privacy Law & Technologies

2020/1

G. Giappichelli Editore

European Journal of Privacy Law & Technologies

Directed by Lucilla Gatt

2020/1

G. Giappichelli Editore

European Journal of Privacy Law & Technologies
On line journal
Italian R.O.C. n. 25223

G. GIAPPICHELLI EDITORE - TORINO
VIA PO, 21 - TEL. 011-81.53.111 - FAX 011-81.25.100
http://www.giappichelli.it

The Journal is one of the results of the European project TAtoDPR (Training Activities to Implement the Data Protection Reform) that has received funding from the European Union's within the REC (Rights, Equality and Citizenship) Programme, under Grant Agreement No. 769191.

Published Online by G. Giappichelli in June 2020
www.ejplt.tatodpr.eu

DATA PROTECTION LAW: A COMPARISON OF THE LATEST LEGAL DEVELOPMENTS IN CHINA AND EUROPEAN UNION

Riccardo Berti
Lawyer at Zumerle Law Firm (Verona, Italy)

Abstract:

The evolution of Data Protection Law in recent years has registered pivotal steps ahead both in China and in the EU.
While the European Union issued the GDPR (Regulation 679/2016), which came into force on 25 May 2018, in China the Cybersecurity Law received major updates and upgrades, among which, on 29 December 2017, the Standardization Administration of China issued the 国标 (guobiao) GB/t 35273-2017 (now GB/t 35273-2020), called 'Personal Information Security Specification' that came into effect on 1 May 2018, recently revised.
Other than the similar date of applicability, the two set of rules share many overlapping dispositions, that witness the growing concerns in this field that both E.U. and China share.
Despite being similar in the form, these rules then vary in the substance.
Therefore, comparing these laws, declined in their respective context, can be useful in order to determine how the right to privacy and data protection is intended in these two legal systems and why some of the European rules have been adopted more leniently in China.

Key-words: Chinese Law, EU Law, Data Protection Law.

sent" in China and in the E.U. – 4.6. The Person in Charge of Network Security and the Data Protection Officer: similarities and differences. – 4.7. Personal data protection Law and Big Data. – 5. Conclusions. – 5.1. Personal Data Protection Law as a tool to rule a global phenomenon. – 5.2. The challenges on the horizon.

1. Introduction

The legal concept of privacy evolves from the so-called "right to be let alone", and was first theorized in 1890 the United States, when jurists Samuel D. Warren and Louis Brandeis wrote 'The Right to Privacy' [1], an article where the phrase "right to be let alone" was used as a definition of privacy.

The article was a response to the worrisome technological developments of the time, such as photography and sensationalist journalism, that posed new types of threats to one person's intimacy.

Since then, the concept of privacy evolved and take broader shape, developing along concepts such as personal information control, the right to be forgotten, big data, etc.

Nowadays, privacy has become a complex concept, difficult to define and with uncertain boundaries [2], that defines the 'claim of individuals, groups, or institutions to determine for themselves, when, how and to what extent information about them is communicated to others'. [3]

The development of this complex concept revolves around concurrent ideas, that see privacy as an evolution of these entitlements: '(1) the right to be let alone; (2) limited access to the self; (3) secrecy; (4) control of personal information; (5) personhood; and (6) intimacy'. [4]

While the privacy concept encompasses mostly a series of prohibitions on interference, from this same concept opened out the idea of a pro-active and dynamic way of safeguarding personal data flows, something more than a simple prohibition. [5]

From privacy therefore grew the concept of personal data protection (spawn

[1] SD Warren, L Brandeis, 'Right to Privacy' (1890-1891) IV, Harv. L. Rev.

[2] D Mulligan, C Koopman, N Doty, 'Privacy is an essentially contested concept: a multi-dimensional analytic for mapping privacy' (2016) 374.118 Phil. Trans. R. Soc. A.

[3] A Westin, 'Privacy and Freedom' (1967) 166 Wash. & Lee L. Rev.

[4] D Solove, 'Conceptualizing privacy' (2002) 90.4 Cal. L. Rev. 1132-1140, D Solove, *Understanding privacy* (Harvard University Press, 2008).

[5] S Rodotà 'Data Protection as a Fundamental Right' in S. Gutwirth, Y. Poullet, P. De Hert, C. de Terwangne, S. Nouwt (eds) *Reinventing Data Protection?* (Springer, 2009), 77 - 82.

from the privacy "facet" of the 'control of personal information'), this is a notion at the same time broader and more specific than the one of privacy, that involves securing data against unauthorized access, sets limits to the power of others on one's personal data and grants right to data subjects in order to limit or call off the processing of their personal data.

Interestingly enough, exactly as it happened in 1890, other worrisome and uncharted innovations set the start for the latest innovations on the privacy/data protection field. For example, in the European Union the spread of Internet marks the basis for the Directive 95/46/EC of 24 October 1995, that sets common principles for European countries in the field of data protection.

More recent developments are motivated by unforeseen threats to individual privacy, compromised by the development of a real "personal data market", where the bidders are social networks and other web giants. In the light of these developments, both E.U. and China issued new legislation in the field.

The European Union issued the GDPR (Council Regulation (EU) 679/2016 of 27 April 2016), which came into force on 25 May 2018, a Regulation that repeals Directive 95/46/EC and deepens the involvement of E.U. in the privacy field.

In China, the Cybersecurity Law received major updates and upgrades, among which, on 29 December 2017, the Standardization Administration of China issued the 国标 (guobiao) GB/t 35273-2017 (now GB/t 35273/2020), called 'Personal Information Security Specification' that came into effect on 1 May 2018 and was recently revised (thus proving the high interest of Chinese government for the subject).

The truth is that, as technology advances, the ways to threaten one person's data changes. Our increasing ability to share information entails that a personal data violation is no more a local problem but can affect the life of one individual everywhere he or she goes, for the rest of his or her life.

These new laws try to address this phenomenon, let's see if their different approaches can cope with the complex technological issues they are facing.

Regarding the Chinese personal data protection law, it is, then, important to stress that the latest intervention on the subject is a 国标 (*guobiao)*. The *guobiao* (literally "national standard") is a peculiar kind of technical legislation that rules many important fields in China. *Guobiao* can be distinguished by the letters accompanying the number and year identifying them. While the acronym "GB" (*Guobiao)* stands for a mandatory provision, a "GB/t" identifies a recommended provision, where the "t" stands for *tuījiàn* ("recommended" in Chinese).

The 'Personal Information Security Specification' (GB/t 35273-2017) is therefore a recommended standard, but its significance in China is greater than

in other nations, because of the rather unique framework of legal formants in the country.

1.1. Method Note

The examination of the declination of an institution belonging to a legal culture that is autonomous, independent and original as the Chinese one is surely suitable for a comparative methodology.

Furthermore, the Chinese example is rather unique. Suffice it to say that China is one of the few countries in the world that did not suffer a direct colonization by a western country [6], thus offering a research environment not affected by the superstructure of a legal system imposed from above by a western power. The colonial period has in fact, willing or unwilling, tamed many other countries to a western legal framework, watering down their original traits. Therefore, we can still find preserved peculiar institutes in China, a country with a rich and millennial legal tradition.

The basis for comparison is without any doubt the European Union, since Chinese legislation in the field has many common traits with the European one, and since both countries decided (around the same period) that they need a revised and comprehensive legislation on privacy and personal data protection.

In order to study the Chinese legal system, which is so unique and so different from western models, we should first set up a method.

In particular this study takes into consideration the theories of Rodolfo Sacco about "legal formants" [7].

The theory of "legal formants" argues considering the role and hierarchy of the law sources in the country subject to study. Sacco evaluates the legislative, legal, and doctrinal "formants".

The different influences of these "formants" in China, as compared to the Western reality, are essential to understand the present and the future of privacy in the country. Dealing with the People's Republic of China, we must acknowledge the importance of the political formant, despite that it very often acts through the three traditional formants indicated by Sacco, it has a specific

[6] Along with Japan, North Korea, South Korea, Nepal, Bhutan, Thailand, Turkey, Saudi Arabia, Iran, Afghanistan, Ethiopia and Liberia.

[7] R Sacco, 'Legal Formants: A Dynamic Approach to Comparative Law (Installment I of II)' (1991) 39 The American Journal of Comparative Law 1, 34; Rodolfo Sacco, 'Legal Formants: A Dynamic Approach to Comparative Law (Installment II of II)' (1991) 39 The American Journal of Comparative Law 343, 401; Rodolfo Sacco, 'Mute Law' (1995) 43 The American Journal of Comparative Law.

weight in Chinese law regardless of its integration into the legal system as it is understood in the West.

Secondly, the tradition, particularly the Confucian one, is considerable according to the classification proposed by Sacco as a "cryptotype" [8], since it certainly contributes to form the mentality of the Chinese jurist, although being unspoken. Another invasive "cryptotype" is surely the one represented by the economic drive, that is behind numerous rules also in the privacy field both in E.U. and in China.

Keeping in mind the role of the political formant and of these "cryptotypes" we can contextualize the noteworthiness of the comparison between China and the European Union in the privacy field. Even if the latest Chinese rules about privacy and data protection, as we have seen, were included in a mere recommended standard, their significance is greater than it would have been in any other country and they have, in fact, already bore an impact in the field, that provides food for thought in this comparison.

Chinese Law in fact often relies on vague core principles, detailed in non-binding rules. This method is really useful for the government since it let to adjust the rule in its practical implementation and to keep it up-to-date without rewrite the law.

The obvious counterpoint of this method is the uncertainty of the law, and the need of some sort of a canister for the population to understand the real weight of a rule.

1.2. Terminology

When dealing with privacy it is important to set straight what do we mean, in both the countries examined, when we talk of privacy, data protection and personal data protection.

As we have seen, privacy evolved from the so called "right to be let alone", to become a complex concept, with uncertain boundaries.

The core meaning of privacy in the legal field is, still today, the exclusion of

[8] A "cryptotype", as defined by Sacco in his *Introduzione al Diritto Comparato* (5th edn, UTET 1992), is: 'a model not verbalized, that was regarded into unexpressed'. The relationship between "formants" and "cryptotypes" is described in the same work: 'of all the formants previously considered here, some are born already verbalized (e.g., the doctrinal formant is closely connected with verbalization), but others are not verbalized at all. We will call 'cryptotypes' these implicit models, the importance of which is immense. The man constantly practices rules that he is not fully aware of, or which, however, he would not be able to express well' [Italian in original text].

unwanted intromission in a subject's life, so it can be defined as a "negative right". On the other side, data protection is the legal control over access to and use of data (regardless the fact that those data qualify as personal data or not). Finally, personal data protection (generally referred to as "personal information protection" in China) is the fraction of data protection that regards personal data (and includes, for example, data security processes, the rules regarding data breaches and how to deal with them, and so on).

By simplifying we can imagine, therefore, a Venn Diagram where the two sets "Privacy" and "Data Protection" overlaps in the "Personal Data Protection" set.

These three concepts are often intertwined and intersecting, and sometimes are used as synonyms, especially when dealing with privacy laws and regulations where, according to the case, the concept of privacy or the concept of data protection is stretched in order to include the other. It is therefore important to understand what privacy, data protection, and personal information protection are in the vocabulary of E.U. and Chinese lawmakers.

In the E.U. we can clearly define two distinct set of "rights" pertaining respectively to privacy and personal data protection [9] that differ in formulation and scope.

While privacy can be identified with the right to respect for private life, the protection of personal data is viewed as 'a modern and active right, putting in place a system of checks and balances to protect individuals whenever their personal data are processed' [10].

Despite this, in the E.U. the term "data-protection" is a term that identifies personal data protection related laws and, sometimes, privacy related laws.

So, we have the 1995 Data Protection Directive and the General Data Protection Regulation in 2016, despite the fact that these legislations involve only personal data protection and privacy (interestingly enough, the term privacy is never mentioned in GDPR).

In China, we have a clearer distinction between the concepts referred, and in fact the General Rules of the Civil Law [11] discipline in two different articles the right of privacy (Article 110) and the protection of personal information (Article 111) [12]. Data protection is instead mentioned by Chinese lawmakers in the Cy-

[9] Source: https://fra.europa.eu/en/publication/2018/handbook-european-data-protection-law-2018-edition Last accessed on September 2020.

[10] ibid.

[11] 中华人民共和国民法总则 (General Rules of the Civil Law of the People's Republic of China), adopted at the 5th Session of the 12th National People's Congress of the People's Republic of China on March 15, 2017 and effective since 1 October 2017.

[12] The Chinese Civil Code, which will come into force in January 2021, maintains the same distinction, defining privacy in Article 1032 and Personal Information in Article 1034.

bersecurity Law, a discipline aimed in fact to protect data regardless of their connection to a natural person.

Here we will examine both privacy and data protection concepts, as long as they are comprised in the recent legal developments examined. In particular, we will examine data privacy and data protection, on one side as developed in GDPR and on the other side as developed in the Guobiao GB/t 35273-2017.

2. Privacy and Personal Data Protection in E.U. Law.

The European Union issued in 2016 the General Data Protection Regulation (Reg. 679/2016), a comprehensive legislation on the personal data protection subject, one of a kind, seeking 'effective protection of personal data throughout the Union', via 'the strengthening and setting out in detail of the rights of data subjects and the obligations of those who process and determine the processing of personal data'. [13]

This result has grown out a long and articulated journey that originates in initiatives of individual EU Member States [14] and in supranational actions, some of which dates back to the 1950s. We shall examine this evolution.

2.1. Evolution and Arrangement.

The first step that led to the current E.U. privacy legislation was the European Convention on Human Rights (ECHR) [15], signed in Rome on 4 November 1950, that states, in Article 8, as follows:

'(1) Everyone has the right to respect for his private and family life, his home and his correspondence.

(2) There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.'

This formula bears, *in nuce,* the fundamental concepts of European privacy

[13] Recital 11 Reg. (EU) 679/2016.

[14] For example, the French Act No. 78-17 on Information Technology, Data Files and Civil Liberties adopted on 6 January 1978.

[15] All the Member States of the E.U. are also signatories of the ECHR.

law, where everyone should be granted the right to respect for his privacy, but this is not 'an absolute right; it must be considered in relation to its function in society and be balanced against other fundamental rights, in accordance with the principle of proportionality' as is stated, today, by the Recital 4 of Reg. (EU) 679/2016.

After this principle was set, the European Court of Human Rights has given it a broad interpretation in its jurisprudence [16], thus laying the foundations for its codification.

Later on, in 1980, further efforts were made by the Organisation for Economic Co-operation and Development (OECD) [17] in order to create a comprehensive data protection system throughout Europe and the U.S., with the adoption of the 'Recommendations of the Council Concerning Guidelines Governing the Protection of Privacy and Trans-Border Flows of Personal Data'.

The OECD Guidelines, however, were non-binding, and data protection laws still varied widely across Europe, with the U.S. and other OECD Member States that, while endorsing the principles within the recommendations, did not implement them in their laws.

In 1981 another institution parallel to the European Community intervened in the matter.

The Council of Europe [18] negotiated within its members the "Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data" (Convention 108) [19]. This convention (still in force) obliges the signatories to enact legislation concerning the automatic processing of personal data, which many of the ratifying countries did.

The Convention 108 is really important also because it sets the boundaries between the privacy right and the personal data protection right(s). Later on, in fact, Advocate General Sharpston claimed, in a privacy related case before the Court of Justice of the European Union, that 'two separate rights are here invoked: "a classic right (protection of privacy under Article 8 ECHR) and a more modern right (the data protection provisions of Convention No 108)." [20]

---

[16] See, e.g., *Klass and others v. Germany*, 6 September 1978, Series A no. 28; *Kruslin v. France*, 24 April 1990, Series A no. 176-A; *Huvig v. France*, 24 April 1990, Series A no. 176-B; *Niemietz v. Germany*, 16 December 1992, Series A no. 251-B.

[17] The OECD reunites 36 countries, among them there are most of the European countries, the U.S., Canada, Chile, Australia, and others.

[18] The Council of Europe is an international organization founded in 1949 that has 49 Member States (all the members of the European Union and several others, including Russia), it operates several international treaties, among which there is the European Convention on Human Rights.

[19] European Treaty Series (ETS) No. 108 – 1981.

[20] CJEU, Joined cases C-92/09 and C-93/02, Volker und Markus Schecke GbR v. Land Hessen, Opinion of Advocate General Sharpston, 17 June 2010, par. 71.

Meanwhile some problems began to emerge, since many European countries had issued legislation in the privacy sector [21], but these laws differed in approach and procedures. This state of things could impede the free flow of data within the European Community. The European Commission decides, therefore, to step in to harmonize the various rules.

The outcome of these efforts was the Data Protection Directive (Council Directive 95/46/EC of 24 October 1995), that was the pivotal European law in the field until 2018. At the time, the European Commission deemed appropriate to issue a Directive [22] since the field was still unripe for a more active participation of the European Community and it was reasonable to let each E.U. Member State to deal with the privacy matter according to its own criteria.

Despite that, the Data Protection Directive contains many of the rules that still govern privacy and personal information protection in the E.U., the directive set the principles of consent, transparency, proportionality, and legitimate purpose for personal data processing. The same law stated the fundamental difference between a data transfer inside the European Union and outside that (transfer of personal data to third countries) and identified the role of supervisory authorities, that are now the cornerstone of data protection implementation and control.

Almost twenty years later, in 2012, the European Commission announced that it would try to unify data protection law across European Union via a proposed legislation called "General Data Protection Regulation" (GDPR).

After an articulated procedure, Regulation (EU) 679/2016 was adopted in 2016 and is applicable from 25 May 2018. This new law supersedes the 1995 Directive and is a significant step forward in the harmonization of privacy law across Europe. While the data protection law set by the European Parliament and Council in 1995, was a Directive, the 2016 law takes on the form of a Regulation, and the choice is all but casual.

In the E.U. hierarchy of laws [23], a Regulation is in fact a far more impactful

---

[21] The first law on data protection was adopted in the German state of Hesse in 1970. Later on, in 1973, Sweden become the world's first nation to enact a data protection law (Datalagen, 1973:289).

[22] A directive has not binding legal force throughout every EU Member State, these instruments lay down certain results that must be achieved by Member States, but each one is free to decide how to transpose directives into national laws. Regulations, on the contrary, have binding legal force throughout every Member State and enter into force on a set date in all the EU.

[23] Article 288 of the Treaty on the Functioning of the European Union states: 'To exercise the Union's competences, the institutions shall adopt regulations, directives, decisions, recommendations and opinions. A regulation shall have general application. It shall be binding in its entirety and directly applicable in all Member States. A directive shall be binding, as to the result to be achieved, upon each Member State to which it is addressed, but shall leave to the national authorities the choice of form and methods'.

set of rules, being directly applicable -as is- in every Member States of the European Union, while a Directive has not binding legal force throughout every EU Member State, merely requiring Member States to reach certain goals, leaving to each state the choice on how to do it and leaving, therefore, potential broad differences in the law from one state to another.

2.2. The Framework of Regulation (EU) 679/2016

On 25 January 2012, the European Commission announced its intention to revise the 1995 data protection directive, in order to update it in the light of technological progress and globalization. [24]

In view of the growing importance of data protection, and in order to guarantee the free movement of data inside the E.U., the aim of this new legislation was also the harmonization of 27 national data protection regulations into one unified Regulation.

Since its original proposal, the European Commission also made clear that the Regulation would apply for all non-E.U. companies active in the E.U. market and offer their services to E.U. citizens.

Later on, after four years of refinement, the General Data Protection Regulation (GDPR) was finally adopted. The GDPR entered into force on 27 April 2016, but has set a compliance date of 25 May 2018, giving E.U. Member States and businesses time to prepare for compliance.

The law is composed by 173 recitals and 99 articles. Recitals, mere interpretative tools of E.U. law, set many relevant principles in European privacy law, useful in order to comprehend how to actually apply its rules.

This preponderance of recitals over articles tells us a lot about the issues encountered by the European legislator in disciplining the complex phenomenon of data protection. Governing privacy with a single law for billion dollars corporations as well for micro-sized businesses, for hospitals and for little sports clubs, for small local authorities and for national ministers, is surely a hard task.

Therefore, European lawmakers resorted to a wide spectrum of quasi-binding principles to guide the application of the fewer rules that reached consensus, for example, an inspiring principle of the new law can be found in its Recital 4, which states that: 'The processing of personal data should be designed to serve mankind'.

Recital 6, instead, explain why it has proved necessary to draft an E.U. Reg-

[24] Source: https://europa.eu/rapid/press-release_IP-12-46_en.htm?locale=en Last accessed on September 2020.

ulation on privacy, saying that: 'Rapid technological developments and globalization have brought new challenges for the protection of personal data. The scale of the collection and sharing of personal data has increased significantly. Technology allows both private companies and public authorities to make use of personal data on an unprecedented scale in order to pursue their activities'.

Other relevant principles can be found in Recital 39, which is like a manifesto for data processing under the GDPR and begin by saying that 'any processing of personal data should be lawful and fair. It should be transparent to natural persons that personal data concerning them are collected, used, consulted or otherwise processed and to what extent the personal data are or will be processed'.

As for the actual rules, the Regulation has its fulcrum in the discipline of the information and access to personal data (Articles 13 and 14 of the Regulation). The law provides a set of mandatory information that the data controller must provide to the data subject when the data are obtained. This information need to be simple and clear (especially when the subject is a minor) and has to explain thoroughly why the data are collected, by whom, how they will be used, how long they will be stored, which are the rights of the data subject and other information in accordance with the specific situation.

It is interesting to note that GDPR contains a broad definition of 'processing', that includes, according to Article 4(2) of the law:

'any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction'.

GDPR then makes a fundamental distinction between "common" personal data and "special categories" of personal data. The latter, disciplined in Article 9 of the Regulation, are data that can reveal 'racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership' and 'genetic data, biometric data, data concerning health or data concerning a natural person's sex life or sexual orientation'. These data can only be processed with particular cautions and with the consent of the data subject (or in some other limited circumstances).

As for "common" personal data, Article 6 of GDPR lists the legal basis for personal data processing as follow:

a) consent from the data subject;
a) performance of a contract;
b) compliance with a legal obligation to which the controller is subject;
d) protection of vital interests of the data subject or of another natural person;

e) performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;

f) legitimate interests pursued by the controller or by a third party.

Among these, the last one mentioned is particularly interesting. Legitimate interest is described by the interpreters as a sort of "wild card" that justifies data processing (though in some limited cases) even if the data subject did not consent to the processing nor to a contract (the Article 29 Working Party [25] states, in its Opinion 06/2014 adopted on 09.04.2014 [26], that the legitimate interest could justify, for example, a re-offer from a producer with whom a data subject has already concluded a sale, or even a limited profiling activity on customers in order to perfect the search for what they have requested). This basis for processing is built on the interest pursued either by the controller or by a third party, therefore, the interest of the data subject does not come into play when dealing with legitimate interest.

The regulation then provides key figures of data controller (the one who processes the data), data processor (the one that, as in Article 28 of GDPR, carries out processing on behalf of a controller), and the brand-new figure of the Data Protection Officer.

This role has to be appointed only if the data controller is a public authority (except in the case of a court), if it performs regular and systematic monitoring of data subjects on a large scale, or if it processes special categories of data on a large scale.

When appointed, the Data Protection Officer (DPO) acts as a *trait d'union* between the business and the supervision authority, it has to be salaried by the business but is "designed for betrayal", as one of its role is to monitor compliance with GDPR by the data controller and to cooperate with the supervisory authority.

Other significant innovations brought by Reg. (EU) 679/2016 in the E.U. privacy and personal data protection framework, are a discipline for codes of conducts and certifications, a new set of rules for data transfers outside the E.U., a new advisory body composed by representatives of the supervisory authorities of each Member State and of the European Data Protection Supervisor, which is called the European Data Protection Board (EDPB) [27], and, eventually, incisive sanctions.

---

[25] Article 29 Working Party was an advisory body, constituted semi-spontaneously under the umbrella of Article 29 of the Data Protection Directive, and reunited a representative from each data protection authority across E.U.

[26] Source: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf Last accessed on September 2020.

[27] Disciplined in Article 68 of Reg. (EU) 679/2016, the EDPB supersedes Article 29 Working Party.

In this regard, Article 83 of Reg. E.U. 2016/679 provides two set of fines. The first one, for lesser violations, features administrative fines up to 10.000.000 EUR, or in the case of an undertaking, up to 2% of the total worldwide annual turnover of the preceding financial year, whichever is higher.

The second one features administrative fines up to 20.000.000 EUR or, in the case of an undertaking, up to 4% of the total worldwide annual turnover of the preceding financial year, again, whichever is higher.

One of the most frequent criticism made of the former Data Protection Directive was in fact the leniency of its sanctions, when dealing with giant multinational corporations; with the new set of sanctions provided by GDPR, anchored to the total worldwide turnover, this risk is fully averted.

2.3. The Dualism Between E.U. Law and Member State Law

With the GDPR, the European Union sought to overcome the limits of the Data Protection Directive, pushing further ahead the harmonization of E.U. states on personal data protection. Despite these efforts, there are many aspects of personal data protection law that are still preserve of individual Member States.

The first example is relative to criminal sanctions. Criminal Law is usually a sensitive area, where Member States sore tolerate meddling by E.U. authorities. Also, in the field of privacy the GDPR is content with its incisive administrative sanctions and does not provides for criminal penalties (as explicitly stated in Recital 149 and in Recital 152 of the Regulation).

A second example regards posthumous data protection. As stated in recital 27 of Reg. (EU) 679/2016, E.U. personal data protection law does not apply to the personal data of deceased persons. However, Member States may provide for rules regarding the processing of personal data of the departed.

Some Member States (for example Italy [28] and Estonia [29]) chose to grant protection to personal data even after the death of the data subject, thus reshaping privacy law and posing new complex questions (who can exercise the right of

[28] Italian *Codice in materia di protezione dei dati personali* (Code regarding the protection of personal data) D.Lgs. n. 196/2003, amended in 2018, states in Article 2 *terdecies* that privacy rights must be granted also to deceased persons, and may be exercised by family members for reasons deserving protection.

[29] Estonian Personal Data Protection Act (RT I, 04.01.2019, 11, available here: https://www.riigiteataja.ee/en/eli/523012019001/consolide last accessed on September 2020) was adopted in 2018 and states, in §9, that the successors of the deceased can object to the processing of his or her personal data for 10 years after the death (20 years if the deceased was a minor).

the dead and whether he or she gain access to all the information possessed by the deceased, even if he or she did not express prior consent to their exposition?).

Moreover, each Member State has adopted a more or less thorough legislation covering privacy, and these laws must cohabit with GDPR and respect its principles.

When dealing with E.U. privacy and personal data protection law, therefore, we should bear in mind that we are talking of a complex and ramified system, unified in its (vague) principles, harmonized in its (few) rules, and diverse detailed rules across the Union.

3. Privacy and Personal Data Protection in Chinese Law

The modern concept of privacy originated in the West [30]; China, exposed to it only in recent times, developed a new word to express the concept: *Yinsi* (隱私). [31]

Despite this, China has had a concept comparable with the one of western privacy through its history. Although Confucian philosophy highlights common and shared values, personal privacy has always been important in China and was guaranteed and even 'valuable in valuable in particular contexts'. [32]

In fact, the same Confucius, in his Analects, stigmatize 'improper' gossip or hearsay [33], and this lead some scholars to argue that the protection of privacy was firstly stated in China by the philosopher of the 6th century BC. [34]

---

[30] 'The conditions for the existence of modem privacy began to form after the Chinese "reform and open" movement in late 1979, with the reform of the economic system. The market changed the face of China.' in J. Cao, 'Protecting the Right to Privacy in China' (2005) 36 Victoria University of Wellington Law Review 647.

[31] 'It appears that the word yinsi is a recent neologism whose use has been heavily influenced by exposure to both Western legal scholarship and popular culture in the mid- to late- '80s (Zhu, 1997; McDougall, 2004)' in Kenneth Neil Farrall, 'Global Privacy in Flux: Illuminating Privacy across Cultures in China and the U.S.' (2008) 2 International Journal of Communication 993, 1030. 'The author believes that privacy was protected, to some extent, in ancient China and an awareness of privacy may be found in the Warring States Period, though neither the word "privacy" (yinsi) nor the modem concept of privacy existed.' in J Cao, 'Protecting the Right to Privacy in China' (2005) 36 Victoria University of Wellington Law Review 647.

[32] Kenneth Neil Farrall, 'Global Privacy in Flux: Illuminating Privacy across Cultures in China and the U.S.' (2008) 2 International Journal of Communication 993, 1030.

[33] Hao Wang, 'The Conceptual Basis of Privacy Standards in China and Its Implications for China's Privacy Law' (2012) 7:1 Frontiers of L in China 137.

[34] ibid.

Chinese contemporary law mentions privacy since in its first Constitution, adopted in 1940, that refers to privacy when affirming protection for correspondence (Article 90, then Article 40 of the new Constitution, adopted in 1982).

But for the development of a real data protection framework in China we have to wait until recent times, when some specific rules where adopted.

3.1. Evolution and Arrangement

The first appearance of a "right of privacy" in China dates to 2002, when a draft of the Chinese Civil Code was reviewed. In the draft, the right of privacy was bordered as follow:

(1) the subject of the right to privacy can only be a natural person;
(2) the objects of the right are private activities and personal information;
(3) the scope of the protection of the right is limited by public interest. [35]

While developing the Civil Code (a process that took eighteen years to be completed), China adopted also some jagged administrative standards, dealing with limited aspects of data protection (e.g.: 'Provisions on Protecting the Personal Information of Telecommunication and Internet Users', adopted by the Ministry of Industry and Information Technology on July, 16, 2013, 'Administrative Measures for Online Trading', adopted by the State Administration for Industry and Commerce on January, 6, 2014, and 'Administrative Rules for Short Messaging Services', adopted by the Ministry of Industry and Information Technology on May, 6, 2015, which regulates marketing activities via SMS).

Perhaps the most relevant administrative standards in the field is the 'Decision on Internet Information Protection' [36] by the Standing Committee of its National People's Congress, which was aimed at protecting "electronic information" and is composed by 12 Articles that contain rules relevant to personal data protection and privacy and that were later on transposed in the Cybersecurity Law.

In the meanwhile, the Supreme People's Court issued some significant judicial interpretations in the privacy field. The first dates back to 1988, when the SPC issued the 'Opinions of the Supreme People's Court on Several Issues con-

[35] Farrall (n. 32).

[36] 全国人民代表大会常务委员会关于加强网络信息保护的决定 (National People's Congress Standing Committee Decision concerning Strengthening Network Information Protection), adopted on 28 December 2012 at the 30th Committee Meeting of the 11th National People's Congress Standing Committee.

cerning the Implementation of the General Principles of the Civil Law of the People's Republic of China (For Trial Implementation)', where the Supreme Court tentatively extended the right to reputation to privacy matters. Then in 1993 the Supreme People's Court issued the 'Reply to Several Questions on Adjudicating the Cases of the Rights of Reputation' and in 2001 the 'Interpretation of the Supreme People's Court Regarding issues of Ascertaining the Liability of Compensation for Spiritual Damage for Tort'.

In 2014, the SPC then issued another significant judicial interpretation, regarding privacy on the web: 'Rules concerning Several Issues in the Adjudication of Civil Disputes over Infringement upon Personal Rights through Information Networks" where the Court deals with the definition of privacy in IT environment, including in its scope genetic information, medical records, criminal records, home addresses and personal activities.

Another relevant Judicial interpretation is the one issued in 2017 by the Supreme People's Court and Supreme People's Procuratorate, called: "Interpretation of Various Issues Concerning Application of Law in Handling Crimes of Infringing upon Citizen's Personal Information". Despite being issued in the criminal law field, the Interpretation clarifies the concept of personal information in China, stating that personal information means any kind of information that, individually or combined with other information, can identify a specific individual. This mean that even a single piece of information (e.g. an IP address, a mobile number, or a license plate) falls within the scope of personal information protection.

After that, the first comprehensive legislation that considered the data protection issue was the China Cybersecurity Law [37], issued on November 7, 2016 and went into effect on June 1, 2017, this law is the outcome of a broader approach to data protection than that adopted by E.U.

While in Europe there is a dedicated law to personal data protection, China favored a discipline aimed at data protection, whether those data are referred to individuals, businesses, etc.

Chapter IV of the Cybersecurity Law (Articles 40-50) deals with 'Network Information Security' and contains many provisions for data protection of citizens online.

The law establishes a right to confidentiality, that shall be respected by network operators (Art. 40) and by departments that deal with cybersecurity supervision (Art. 45), a right to erasure (when network operators have processed data in violation of law, set in Art. 43). Moreover, network operations shall not gath-

[37] GB/t 35273-2017 中华人民共和国网络安全法 (Cyber Security Law of the People's Republic of China) adopted at the 24th meeting of the Standing Committee of the 12th National People's Congress on November 7, 2016.

er user personal information, except when those are processed according to the principles of legality, propriety, and necessity.

Under the scope of the Cybersecurity Law, on April 19, 2019, China's Ministry of Public Security released a 'Guideline for Internet Personal Information Security Protection' (互联网个人信息安全保护指南).

Another pivotal step forward was made with the adoption of the General Rules of the Civil Law, at the 5th Session of the 12th National People's Congress of the People's Republic of China on March 15, 2017 (the law is effective since 1 October 2017).

Article 110 of the General Rules states that natural persons enjoy a list of rights, among which the right to privacy is included.

Then Article 111 of the General Rules stipulates that the personal information of natural persons is protected by law. Any organization or individual who needs to obtain personal information of others shall obtain and ensure the security of the information according to law, and shall not illegally collect, use, process, or transmit the personal information of others, and may not illegally buy, sell, or disclose the personal information of others. This rule constitutes a firm basis in law for the evolution that will take place in this field in China in a near future.

The General Rules will be abolished as soon as the Civil Code of the People's Republic of China (adopted during the 13th National People's Congress on May 28, 2020) will enter into force on January 1, 2021 [38].

The Civil Code includes an entire chapter dedicated to privacy and personal information protection (Chapter 6 of Part IV "Personality Rights", Articles 1032-1039), that further develops the principles contained in the General Rules.

This Civil Code takes up the borders of the 2002 draft and develops the concept in its consequences.

Chapter 6 of the Civil Code opens up with Articles 1032 and 1033, dedicated to the right of privacy. In these articles the law states that 'no organization or individual may infringe upon the privacy rights of others' and lists a series of activities prohibited (except when permitted by law or with the consent of the subject) that includes unwanted calls, text messages, instant messages, e-mails, photographs or films of private life and places, etc.

Article 1034 then defines personal information and states that it is protected by law.

The definition of personal information provided in the same article comprises electronically or otherwise recorded information that can identify a specific

[38] Civil Code of the People's Republic of China (中华人民共和国民法典), Enacting Organs: The 13th National People's Congress on May 28, 2020 in the Diaoyu Islands (at the third plenary session of the Third Session of the 13th National People's Congress), issued on May 28, 2020, effective from January 1, 2021.

natural person individually or in combination with other information (a broad definition that echoes the one contained in Article 4 n. 1) of Reg. EU 679/2016) and include the person's name, date of birth, identity card number, biometric information, address, telephone number, e-mail address, health information, whereabouts information, etc.

When processing personal information, Article 1035 states that the data controller shall follow the principles of lawfulness and necessity and shall be based on the consent of the natural person, unless otherwise provided. Article 1036 then enlists two examples of these provisions that let the processing to happen without consent, the first one is the case of the reasonable processing of information disclosed by the natural person or lawfully obtained, the second one is the case of the reasonable processing of information implemented in order to safeguard the public interest or the lawful rights and interests of the natural person.

It is interesting to note that Article 1037 of the Chinese Civil Code lays down in law the right of access of the data subject, the right to rectification and the right to erasure (that find their counterpart in Articles 15, 16 and 17 of Reg. (EU) 679/2016).

Article 1038 states that data controller shall not disclose or tamper with the personal information they collect or store and that they shall take technical and other necessary measures to ensure the security of the personal information they collect and store. Lastly, Article 1039 declares that even administrative bodies shall keep confidential the personal information of natural persons known in the course of performing their duties, and shall not disclose or illegally provide them to others.

The Civil Code, when it will enter into force in 2021, will surely push forward Chinese personal data protection framework, providing a set of definitions and binding rules that will guide the mandatory standard that will eventually follow the one (GB/t 35273-2017, merely recommended) examined in this article.

In pair with this development, we should expect a personal data protection law to be drafted within 2020 according to the update of the legislative agenda made by the Standing Committee of the National People's Congress of China in September 2018, promising a comprehensive data protection law the end of its term. [39]

[39] Yang Feng, 'The future of China's personal data protection law: challenges and prospects' (2019) 27:1 Asia Pacific Law Review 62-82.

3.2. The Impact of the 'Personal Information Security Specifications'

Another step forward for privacy and personal data protection in China is surely the GB/t 35273-2017 'Information Security Technology Personal Information Security Specification' [40].

This Standard is a Guobiao (literally: "National Standard"). Guobiao are provisions usually issued by the Standardization Administration of China (SAC), that can be distinguished by the letters accompanying the number and year identifying them, specifically, while the acronym "GB" (Guobiao) stands for a mandatory provision, the acronym "GB/t" identifies a recommended provision, where the "t" stands for tuījiàn,

The 'Information Security Technology Personal Information Security Specification' is therefore a recommended standard. Despite its being non-binding, it is particularly interesting for two reasons.

First of all, this Standard has many traits in common with the European GDPR, starting from the date of implementation, set on May 1, 2018, close to the date of applicability of the GDPR (May 25, 2018). [41]

Secondly, the particular layout of the legal framework in China, as seen in the method note, ensures more relevance to this standard, even if it lacks coercive force.

In China the political level, or political "formant" as Sacco would describe it [42], runs parallel to the legislative and administrative levels; the Party still has a significant impact on the decisions taken by other administrative bodies, even if its vision is not yet transposed into law [43]. This entails a situation where the rule of law is not the same as the one known in Western countries but is rather a means for clarity and predictability of the rules of the political leadership, preferable but not necessary. This is the reason why some scholars call the present situation in China 'rule by law' [44].

---

[40] 信息安全技术 个人信息安全规范 (Information security technology - Personal Information security specification) issued by the General Administration of Quality Supervision, Inspection and Quarantine of PRC and Standardization Administration of PRC on 29 December 2017 and implemented on 01 May 2018.

[41] These common traits should not be surprising if we consider that both these rules take their cue from the principles set by a supranational authority, the Organisation for Economic Co-operation and Development (OECD), in 1980.

[42] Sacco (n. 7).

[43] Yuanyuan Shen, ' Conceptions and receptions of Legality: Understanding the Complexity of Law Reform in Modern China' in K. Turner, J. Feinerman, R. Guy, (eds.), *The Limits of the Rule of Law in China* (University of Washington Press, 2000), 20-44; I Castellucci, *Rule of Law and Legal Complexity in the People's Republic of China* (Università degli Studi di Trento, 2012).

[44] I Castellucci, 'Rule of Law with Chinese Characteristics' (2007) 13 Annual Survey of International and Comparative Law 1, 35.

The political relevance of the Standard under consideration is recognized by many scholars [45] and evidenced by the fact that, on February 1, 2019, China's National Information Security Standardization Technical Committee has proposed a set of revisions to the national standard Personal Information Security Specification (ref. GB/t 35273–2017), released for public consultation.

The day after, the China Cyber Security Review Technology and Certification Center announced that some major companies, including Alipay and Tencent, obtained a privacy related certification based on the National Standard. [46]

The Standard sets the principle of explicit consent for the processing (Art. 3.6) referring to the need of "Affirmative Actions" (*kěndìng xìng dòngzuò,* 肯定性动作) in order to process data, as happens in GDPR (Recital 32).

Then the Chinese Standard provides a subdivision of personal data in 'common' data and 'sensitive' data. Sensitive data are defined, in Article 3.2, as data that, once leaked, can threaten personal and property security or easily cause personal reputational damage, physical and mental health damage, or discrimination. [47]

It is interesting to note that, contrary to what does the E.U. law, sensitive data are defined not by category, but by the negative effects of a potential data leak.

The Specification defines also anonymization and de-identification, saying that the anonymization is an irreversible process that does not consent to recover personal data, while de-identification is a process that allows to identify the data subject with the use of additional information (this concept is comparable with pseudonymization, as defined in GDPR).

The rule stipulates that information produced by anonymizing personal data does not qualify as personal data. As the Civil Code, also this Standard discipline the right of access, to rectification and to erasure (Art. 7.4, 7.5, 7.6 respectively). The right to erasure does not seem as developed as its European counterpart, since in the E.U. right of erasure is a genuine right to be forgotten, not pegged to any violation of law (requested for the deletion according to GB/t 35273-2017 Art. 7.6).

---

[45] Emmanuel Pernot-Leplay, 'China's Approach on Data Privacy Law: A Third Way Between the U.S. and the E.U.?' (2020) 49:8 Penn St J L & Int Aff 74 (The role of non-binding rules).

[46] Source: https://equalocean.com/fintech/20190203-fintech-giants-acquire-crcc-certifications-on-private-information-security Last accessed on September 2020.

[47] The Standard also provides a list of examples of what could constitute a "sensitive" data: identity card numbers, biometric information, bank account numbers, communication records and contents, property information, credit information, location data, accommodation information, health and physiological information, transaction data, and any data regarding people of 14 years of age or under.

Another interesting definition, contained in the Standard, is the one regarding automatic decision making; when making decisions that significantly affect the subject matter of a personal data subject based solely on the automatic decision-making of the information system (e.g., determining personal credit and loan quota based on the user profiling, or using the user profiling for interview screening), the personal data controller shall provide a method of appeal to the personal data subject.

This rule is quite like the one adopted by E.U. lawmakers, but both the definitions face numerous criticalities, since it is quite uncommon that a decision on relevant matters could be solely machine-based. In most cases the software aims to facilitate the decision of a human being (who could be heavily influenced by the faith in the algorithm capacities), and therefore both Chinese and E.U. law cannot assist the citizen subject to an algorithm-assisted decision.

Further on, the Standard defines, in Article 8.2, the data processor, and requests the controller to supervise the processing of its delegate.

Another institution comparable with its European counterpart is the Security Incident Notification (disciplined in Article 9.2 of the Standard). As it happens under GDPR, the data controller shall promptly notify data subjects of the data breach (through email, letter, telephone, or push notification). If it is difficult to individually inform the data subjects, the controller should deliver a public warning (in an effective and appropriate manner).

In this case we can notice that the Chinese Standard lacks a supervision authority dedicated to privacy violations, that under Reg. (EU) 679/2016 shall be involved in case of data breach.

GB/t 35273–2017 requires also the appointment of an in-house responsible for data protection for businesses which meet certain requirements (at Article 10.1 b). Specifically, the organizations which main business involve the processing of personal data and have more than 200 employees, and the organizations that process data of more than 500.000 people (the revision raise this threshold to 1.000.000 people) or expect to do so within 12 months shall appoint a responsible for data protection. The responsible for data protection, though, is quite different from the data protection officer covered by GDPR.

The Chinese "responsible for data protection" has the task of coordinate and carry out data protection, to formulate, implement and update a privacy policy, to conduct privacy impact assessments, to enlist the data processing conducted by the business, to organize privacy training, to examine data protection related to new services or products, and to conduct security training. These tasks are the one that, in E.U. law, are assigned to the data controller, that surely can and should be helped by its privacy team in case of complex corporate structures. The data protection officer introduced in GDPR, instead, does not carry out these tasks, but solely oversees data protection in the organization that has ap-

pointed him/her and is a contact point between the business and the supervision authority.

The Standard then contains some surprisingly detailed dispositions, as the one that regulates the display of personal data on message boards, stating that data controllers should take measures in order to obtain the de-identification of data subjects (Article 7.2).

3.3. The recent amendment to the 'Personal Information Security Specifications'

The relevance of the standard examined is evidenced by the fact that soon after its release, on February 1, 2019, China's National Information Security Standardization Technical Committee proposed a set of revisions to the national standard Personal Information Security Specification (ref. GB/t 35273–2017), released for public consultation, eventually adopted on 06 March 2020 under the number GB/t 35273-2020 that will be effective from 01 October 2020[48].

As it often happens in China when a standard is decisively revised, the "amendment" replaces the previous standard, keeping the same number (i.e. 35273) followed by the year of adoption of the amendment (2020).

The modifies include a distinction in the concept of consent, with article 3.6 now split in two; on one side article 3.6 will discipline (from 01 October 2020) the "explicit consent" and on the other side the newly introduced article 3.7 will discipline the concept of "consent" (*recte* "implicit consent") a broader concept that includes negative actions such as not leaving the area (for example a website) after being informed of the data processing.

Also, the definitions of 'personal information' and 'personal sensitive information' are enriched by a note that specify that the definition include personal information "created" by the data controller through processing other information (whether personal or not); the note provides the example of an user profile image (Art. 3.1 and 3.2).

It is then introduced a ban on coercing users to agree to data collection by bundling services (Art. 5.3), and also a much welcomed compulsory "separation" of the consent, requiring different shows of assent for "basic business functions" (*jīběn yèwù gōngnéng* 基本业务功能) and "additional business functions" (*kuòzhǎn yèwù gōngnéng* 扩展业务功能), just like the E.U. law that requires

[48] GB/t 35273-2020 信息安全技术 个人信息安全规范 (Information security technology - Personal information security specification) issued by the General Administration of Quality Supervision, Inspection and Quarantine of PRC and Standardization Administration of PRC on 06 March 2020 and effective from 01 October 2020.

(Recital 32 and 43) 'separate consent to be given to different personal data processing operations' in order to attain a 'freely given' consent.

The revision also adds Appendix C.1, C.2, and C.3, regarding the definition and the distinction between "basic business functions" and "additional business functions".

The same revision adds Article 7.5 to the Standard, this Article sets the requirements for "personalized displays" (e.g. newsfeeds and search results personalized depending on the user identity), and it is stated that a clear mechanism of opt-out has to be made available for users. Moreover, personalized displays shall be clearly identified with the words "targeted push" (*dìng tuī* 定推) marked in a prominent way.

Then the renewed Article 7.6 will require that the convergence of personal information collected on different legal basis shall in any case respect the limits of processing set by the Standard.

Another significant innovation is brought about by the introduction of Article 9.7, that governs data access by third parties. The Article requires a security access mechanism between the controller and the third party (if deemed necessary) and the fact that the third party shall obtain the authorization to collect personal information from the data subject (this authorization to the access of a third party, in accordance with the relevant provisions of the Standard, can also be obtained in advance by the original data controller).

If data acquisition by a third party is embedded to an automation tool (such as codes, scripts, interfaces, algorithm models, software development kits, applets, etc.) the data controller shall carry out technical testing to ensure that the data collection comply with the agreed purpose and immediately disconnect them if the data collection exceeds the same purpose.

The revision then provides detailed provisions regarding biometric information and their processing. The renewed Article 6 includes various precautions to adopt when dealing with biometric information (*gèrén shēngwù shìbié xìnxī* 个人生物识别信息).

For one thing, Article 6.3 lett. c) states that biometric information should not be stored, but rather collected only instantaneously collected for authentication purposes and then discarded (e.g. with a dedicated collection terminal).

If the storage is essential for the processing purpose, Article 6.3 lett. b) requires separate storage for biometric information and personal identity information.

Article 9.2 lett. i) then states that personal biometric information may not be shared or transferred to third parties, unless the sharing or transfer is essential for the processing purpose.

As anticipated, the revision of Article 10.2 of the Standard also raises the threshold for the obligation to appoint a responsible for data protection.

The revision then introduces the so-called "Personal Information Security Project" (*gèrén xìnxī ānquán gōngchéng* 个人信息安全工程) that, much akin to the principle of "privacy by design" present in Reg. (EU) 679/2016 (Art. 25), states that data controllers should consider personal information protection requirements at the stage of system engineering, in order to ensure the protection of personal information during system construction.

Lastly, the revision introduces Article 11.3, where are disciplined the 'Records of personal information processing activities', much akin to the 'Records of processing activities' disciplined by Article 30 of Reg. (EU) 679/2016. The same article 10.2 of the revised Standard says that it is 'advisable' to adopt such records. As in the E.U. privacy framework, these records could be a useful instrument for mapping data processing and identify weak spots that need refining.

The revision is a positive step in the right direction, reinforcing the freedom of consent and advising organizations to keep records for data processing.

The only downsides in the revision that will come into force on 01 October 2020 are the introduction of the so-called "implicit consent" (that weakens the safeguards for the data subject) and the increase in the threshold for the appointment of a responsible for data protection (from the data processing of 500.000 people to 1.000.000 people)[49]; it is in fact difficult to believe that a corporation that processes data of more than 500.000 people is not in need of a subject dedicated to ensure the safety of that processing.

On the contrary it is to be welcomed the introduction of another threshold for the appointment of a responsible for data protection consisting in the processing personal sensitive information of more than 100,000 people (albeit, again, too high). [50]

3.4. Latest regulations

Other recent innovations in China bear witness to the increasing importance of privacy in the country.

Various Chinese authorities have in fact begun to take action in the field, in a script that has already been recited in other fields: when the central political level in China is ready for an innovation, before the finalisation of a law, many governmental agencies and local authorities begin to test its principles and effects. [51]

---

[49] Article 10.2 lett. C) (2) of GB/t 35273/2020.

[50] Article 10.2 lett. C) (3) of GB/t 35273/2020.

[51] A useful example can be found in the environmental field, as seen in: Mariagrazia Sempre-

The first example is a so called "privacy seal", announced on 15 March 2019 by the State Administration for Market Regulation and the Office of the Central Cyberspace Affairs Commission and called 'Mobile Internet Application (App) Security Certification Implementation Rules'. The China Cybersecurity Review Technology and Certification Centre will act as the certification authority. The certification is voluntary, but mobile app developers are encouraged to voluntarily obtain this certification, while search engines and app stores are encouraged to give more visibility to certified apps. [52]

On the same topic, on 8 August 2019, the National Information Security Standardization Technical Committee Secretariat issued a notice on the development of a draft of a Guobiao called: 'Basic specification on personal data collection by Mobile Internet Application (App)'. [53]

The standard recalls terms and definitions of GB/t 35273–2017 and comes with an appendix which lists the most common mobile internet application services (the list contains 21 services, such as map navigation app, instant messaging app, and so on) and the minimum information required to provide the service for each category.

Also, some recent court decisions are significant for present purpose, for example Tianjin Binhai New Area People's Court has issued on 20 March 2019 an injunction towards ByteDance (the owner of the renowned video app TikTok), ordering that it immediately stop providing the WeChat/QQ open platform authorised login to its recently launched app Duoshan (a short video-based messaging app), and that the same app must stop using WeChat/QQ user profile photos and nicknames in order to suggest new contacts. [54] The case is still on trial and the ruling will surely address the problem of balancing the interest of consumers to their data protection and to data portability, along with the interest of the two tech giants to hold back and to obtain personal data of their users.

Despite the injunction stems from a competition problem between two tech giants, it is interesting enough to note that this problem would have been avoided if those companies had adopted the Standard GB/t 35273–2017 that imposes, especially after the proposed revision, a complete control for the data subject of

---

bon, 'The Environmental Issue in China: Norms and Enforcement After Cop-21 Climate Summit in Paris' (2016) 3(1) Geoprogress Journal.

[52] Source: https://www.insideprivacy.com/international/china/china-introduces-mobile-application-security-certification-scheme/ Last accessed September 2020.

[53] Source: http://www.cac.gov.cn/2019-08/08/c_1124853418.htm (CN) Last accessed on September 2020.

[54] Source: https://www.tmtpost.com/nictation/3830482.html, https://www.theepochtimes.com/law-professor-sues-chinese-zoo-for-mandatory-face-scanning_3138101.html Last accessed on September 2020.

the data shared (willingly or not) with third parties.

Another very recent case is the one that involved a the Hangzhou Safari Park that switched from fingerprint authentication to facial identification for its visitors to access the park and was sued by one of its customers that was willing to access via fingerprint scanner but not to grant the park his facial identification data. The case was filed on October 28, 2019 and is still pending. [55]

The case has many interesting contact points with an Illinois litigation that was brought before Court in 2014, when an amusement park begun to use fingerprint authentication in place of tickets, leading to the Court ruling against the park and awarding punitive damages to the aggrieved party on January, 25, 2019 [56], despite the law effective in the State (Biometric Information Privacy Act, BIPA) being quite generic on the matter.

Before the Guobiao GB/t 35273/2017 and the Cybersecurity Law, there was a limited case law related to privacy and personal data protection in china, there were some significant criminal cases (among which the Qi Yuling v. Chen Xiaoqi case and the Wang Fei case [57]).

In the Qi Yuling v. Chen Xiaoqi case, Ms. Qi complained that that Ms. Chen stole her identity in order to obtain admission to University "on her behalf". The Supreme People's Court ruled in favor of Ms. Qi on the basis of infringement of her constitutional rights. About the Wang Fei case, we will further examine it in Chapter 3 (Comparison).

Apparently, criminal prosecution was the preferred way for Chinese citizens to protect their rights to their personal information. The Hangzhou Safari Park case is the sign of a recent turnaround. Another element that lately pushed Chinese plaintiffs to turn to the civil judge is the establishment of the so called "Internet Courts". The first Internet Court was set in Hangzhou [58] in 2017 after a stage of pilot establishment and has jurisdiction over the internet-involved civil and administrative cases. In addition to deal with internet-related cases, Inernet Courts benefits from a high-tech procedure (e.g. hearings through video-chat). After Huangzhou, similar courts were established in Beijing and in Guangzhou in 2018. It is clear that many privacy related cases, that nowadays often involve

---

[55] Source: https://www.bbc.com/news/world-asia-china-50324342, https://www.theepochtimes.com/law-professor-sues-chinese-zoo-for-mandatory-face-scanning_3138101.html Last accessed on September 2020.

[56] *Rosenbach v. Six Flags Entertainment Corp.* 123186 (Ill. 2019).

[57] Mentioned in the In-Depth Analysis "The data protection regime in China" by the European Parliament Directorate General For Internal Policies, that can be accessed at the following link: http://www.europarl.europa.eu/RegData/etudes/IDAN/2015/536472/IPOL_IDA(2015)536472_EN.pdf Last accessed on November 2019.

[58] Hangzhou is home to many Chinese high-tech companies, distinctly Alibaba.

networks and technology, will be examined by these specialized courts.

Finally, perhaps the most significant element that shows the growing interest for privacy in China is the fact that a personal information protection law drafting has been included in this term's legislative plan [59] and the space devoted to privacy and personal information protection in the Civil Code recently approved.

In a note issued on the National People's Congress (NPC) website on 6 June 2019, a spokesman confirmed that drafting of personal information protection law has been included in the legislative plan for this term. Reacting to the worrisome issues of the so called "browser home page hijacking" and "mobile app hijacking" (widespread redirect viruses), the spokesman confirmed the illegal nature of these practices and ensured that the National People's Congress is going to intervene in the fragmented legal framework regarding privacy in China. The Standing Committee of the National People's Congress has, therefore, included the drafting of personal information protection law in the legislative plan of this term. [60]

Given the binding legal basis provided by the Civil Code and the seen mechanisms regulating Chinese legislation, it is to be expected that the Chinese personal data protection law will take extensive guidance from the standard examined in this article.

4. Comparison

When dealing with two legal system so different and rich in tradition as the European and the Chinese one, it is important to calibrate the meaning of the legal concepts that we are dealing with, declined over the two legal systems.

Doing this, we see that privacy, in China and in the West, are different concepts. The modern concept of privacy is born in the U.S. and transposed into law in the E.U., while is alien in Chinese culture. However, it does not mean that in China a concept of privacy "with Chinese characteristics" was present since ancient times. [61]

While European Culture values individualism and, therefore, the right to be left alone, Chinese culture traditionally valued social harmony (a Confucian concept recently recalled even by Xi Jinping in his rhetoric [62]).

In order to obtain social harmony, there is the need of a certain knowledge of

[59] Yang Feng (n. 39).

[60] Source: http://www.npc.gov.cn/npc/c199/201906/86e7ca82949844e29f0136b453781ad6.shtml (CN) Last accessed on September 2020.

[61] See Farrall (n. 32) and Wang (n. 33).

[62] E.g. in his report at the 19th CPC National Congress (10.18.2017).

personal data by the same society. This is not necessarily an intrusion in someone's life, but rather a different approach on privacy, where some fraction of oneself data must be exposed for greater good. The same mechanisms apply in E.U. law, as we have seen, where it relies on a balancing of interests in order to decide whether some personal data can be processed or not.

In China this mechanism is different in the way this balancing is set, but this does not mean that E.U.-like law cannot be applied in China, and this explain the reason behind the adoption of a standard (GB/t 35273–2017) so close to the European one.

Eventually, Chinese society will loose those social ties, pressured by economic growth, progressive urbanization, and rural to urban migrations, that put the Chinese social fabric to a severe stress and make communitarianism become less of a necessity and more of a choice. Therefore, privacy will probably take more and more its place in Chinese law, even if, again, "with Chinese characteristics".

Bearing this in mind, we can examine the differences between China and E.U. when dealing with privacy and data protection.

Also, in China privacy is a concept that is limited to the so-called "right to be left alone", whereas the term "personal information protection" subsume personal data protection related laws.

The lexicon of privacy is indeed complex also in Europe, where "privacy" is a term generally avoided by E.U. lawmakers, with the broader term "data protection" used to subsume personal data protection measures and sometimes privacy rules.

In Europe we have a comprehensive legislation, result of a complex and multiannual evolution, that had led privacy to be part of the everyday life of E.U. citizens, businesses and authorities. Although, this set of rules is difficult to implement in a legal framework as complex as the European one, making almost impossible to obtain the same level of adjustment across the Union.

In China we have a peculiar situation, where the law to this day is still fragmented and composed by few specific laws and standards introduced in sector rules. At the same time, there is already a Standard (although recommended) that sets a comprehensive privacy discipline, comparable to that adopted in the E.U.; moreover, at the political level have been taken numerous clear-cut measures that show the concern over the personal data protection issues.

In any case, it will probably take many years to come in order to instill a culture of privacy (from which personal data protection stems) in Chinese organizations and citizens, especially considering the spread of the so-called "human flesh search"[63] in the country, and some recent initiatives by the government

[63] Human Flesh Search (*Rénròu Sōusuǒ* 人肉搜索) defines the phenomenon of a distributed research of personal data (usually driven by social outrage) through Internet media.

(e.g. the so called "Skynet Project"[64], the so called "Social Credit System"[65] and the comprehensive "Smart City Program"[66]) that seem to encourage a data collection focused on quantity over quality, while, on the other hand, European Union requires that also public authorities minimize their data processing.

4.1. The concept of personal data in China and in the E.U.

We have seen that the concept of privacy, personal data/information and data protection varies in the perception of Chinese and European citizens and traditions. It is really interesting, then, to examine how this concept reverberate in each legislation.

Despite only implying it in its name, E.U. Data Protection legislation is actually aimed only at personal data protection. In fact, Article 2 of Reg. (EU) 679/2016 (headed: 'Material scope') states that: 'This Regulation applies to the processing of personal data'.

Article 4(1) of GDPR then states that "personal data" are 'any information relating to an identified or identifiable natural person'. Then the same Article provides a definition for "identifiable natural person", which is 'one who can be identified, directly or indirectly'.

In the Chinese standard (Article 3.1) there is a similar definition, where personal data include: 'all kinds of information, recorded by electronic or other means, that can be used, alone or combined with other information, to identify a specific natural person or to discover activities of a specific natural person.'

As we can see the definitions (and the material scope of the two rules) are quite superimposable, despite the E.U. one being unnecessarily complex (splitting the definition in two: "personal data" and "identifiable natural person").

Interestingly enough, the Chinese definition seems to extend personal data to data related to "activities" of a natural person. Despite this apparent extension, it is clear that these "activities" are no more than a mean to indirectly identify a

[64] Source: http://paper.people.com.cn/rmzk/html/2017-11/20/content_1825998.htm (CN) Last accessed on September 2019, http://www.chinadaily.com.cn/a/201712/12/WS5a2fa4f7a3108bc8c6727f5c.html Last accessed on September 2020.

[65] See: C Yongxi, ASY Cheung, 'The Transparent Self Under Big Data Profiling: Privacy and Chinese Legislation on the Social Credit System' (2017) 12(2) The Journal of Comparative Law 356, 378; M Chorzempa, P Triolo, S Sacks, 'China's Social Credit System: A Mark of Progress or a Threat to Privacy?' (2018) Policy briefs.

[66] See: F Yang, J Xu, 'Privacy concerns in China's smart city campaign: The deficit of China's Cybersecurity Law' (2018) 5 Asia Pac Policy Stud. 533, 543; J Wagner Givens, D Lam, 'Smarter Cities or Bigger Brother? How the Race for Smart Cities Could Determine the Future of China, Democracy, and Privacy' (2020) 47 Fordham Urb. L.J. 829-882.

natural person and that only the possibility of a connection between the activity and the natural person qualify the data as personal data.

Given this, we can see that the starting point of both Chinese and E.U. personal data protection rules is quite the same, thus demonstrating that privacy and personal data protection are indeed universal concepts that varies in the details, but maintains a core meaning across the world.

4.2. The scope of application of GDPR and GB/t 35273–2017

According to E.U. Law (Article 2 of GDPR), the regulation applies to the processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system.

This means that data protection is regulated by Reg. (EU) 679/2016 to a greater extent when the processing is automated, while its scope narrows down if the processing happens by "manual" means, involving only data which form part of a filing system (i.e. a categorized database of personal information).

The same Article 2 of GDPR lists some relevant exceptions to the application of its provisions:

a) activities which falls outside the scope of Union law;

b) activities carried out by the Member States regarding foreign and security policy;

c) activities carried out by a natural person in the course of a purely personal or household activity;

d) activities carried out by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security.

These exclusions are quite relevant and diminish the protection for data subjects in a large series of hypothesis.

Despite the presence of other safeguard measures for the protection of the individuals privacy and confidentiality within E.U. Law, it is clearly compromising that all the comprehensive legislation set in Reg. (EU) 679/2016 cannot be invoked in these cases (e.g. when a person photographs another without his/her consent and spread the image on the web for purely personal reasons, it is difficult to argue that the subject photographed can refer the matter to the supervision authority set in GDPR or call for the application of GDPR fines).

In the Chinese standard the scope of application of the Guobiao is set in Ar-

ticle 1, which states that the standard applies to 'various entities' (*gèlèi zǔzhī* 各类组织), and the processing made when supervising, administering, and assessing the processing activities by supervisory authorities and third-party review organizations.

So, Article 1 clarifies that the scope of the Standard is limited to organizations (companies, firms, associations, and other businesses) and shall be followed also by the public sector and by reviewers when assessing the data processing activities. The rule seems then to self-limit itself to the private sector, stating that the public sector has to follow its rules only when supervising, assessing and administering the processing activities made by the 'various entities' subject to the Standard.

This Standard then is not intended to discipline the data processing made by the Chinese public sector, while the European Regulation is aimed also to Member States and their administrative bodies (except for some particularly sensitive areas, as seen above). It is, obviously enough, a difference that is connatural to the fact that the Chinese Guobiao is a recommended standard, and that the Chinese government will enact and follow its separate specific rules for processing personal data later on. [67] It is interesting to note, though, that this rule would not be capable to curb the phenomenon of human flesh search, [68] since it is not applicable to individuals.

As well, also E.U. law would be inadequate to reach that objective, since it is not applicable to individuals that act for personal means (it is, although, arguable that the collective effort aimed to search for personal data on the web would not fall under the definition of 'purely personal activity').

Other differences arise when examining the types of processing subject to the Standard, with its Article 1 that goes on to state that the Standard applies to the processing of personal data, giving then a non-exhaustive list of types of processing (collection, storage, use, sharing, transfer, and disclosure).

The standard then, seems to be applicable to more kinds of processing when compared to its European counterpart (that excludes manual processing not intended for a filing system).

Here, again, we see that the nature of recommended Standard does not require special care in setting its restrictions, since every voluntary adoption of the Standard is welcomed. The Standard only sets, in Article 1, its intended audience.

Despite the seen differences, it is clear that there are many common traits between the E.U. Regulation 679/2016 and Chinese Standard GB/t 35273-2017.

---

[67] The first rule to usher a liability for administrative bodies that misprocess personal data is contained in Article 1039 of the Civil Code of the PRC, that will come into force in January 2021.

[68] See n. 62.

Both the rules examined, in fact, provide a rather widespread concept of personal data, suitable to include the most relevant processing activities that could undermine personal data of citizens, i.e. the processing made by businesses, that crave for personal data for marketing purposes.

4.3. The information provided to the data subject in China and in the E.U.

Both the E.U. Regulation and the Chinese Standard set a list of information that a data controller shall provide to the data subject when processing his/her personal data. This list is particularly interesting since it details which information is essential, according to each law, in order to allow the data subject to exercise his/her rights.

The European regulation lists the information in Article 13, which states that when the data controller obtains data from a subject, it shall provide all the following information:

– the identity and the contact details of the controller;

– the contact details of the data protection officer, if any;
– the purposes of the processing and the legal basis for the processing;
– the legitimate interests pursued, when the processing is based on it;
– the recipients of the personal data, if any;
– if the controller intends to transfer personal data to a third country or international organization;
– the period for which the personal data will be stored or the criteria used to determine that period;
– the rights of the data subject;
– the rights to withdraw consent, when the processing is based on it;
– the right to lodge a complaint with a supervisory authority;
– if the data subject is obliged to provide the personal data and of the possible consequences of failure to provide such data;
– the existence of automated decision-making, if any, and meaningful information about the logic involved.

For its part, the Chinese standard GB/t 35273–2017 (Article 5.4) requires that controllers shall provide the following information prior to the collection of the personal data (if the collection is subject to the consent of the data subject or when there is an automatic data collection):

– the types of data collected, in relation with the different purposes of the product or service;

– the rules of collecting and using the personal data, among which are:
• purpose of collection and use;
• manner and frequency of collection;
• storage location;
• storage period;
• data security capabilities;
• information related to sharing, transferring, and public disclosure.

It is interesting to note that while the European Law provides that the controller shall give the information when it obtains the data (this rule, in one with the fact that GDPR does not apply to manual processing not intended for its inclusion in a file system, has made possible to argue that the "first contact" between controller and subject does not require immediate information of the latter about the data processing), the Chinese standard is stricter and requires that the controller provides the information prior to the collection of personal data, therefore leaving no room for "first contact" exemption from both consent and information.

Chinese Guobiao also states that, in addition to the seen information (that should be provided when the data are acquired), Chinese data controllers should provide a privacy policy and every data subject should be made aware of its contents (it appears that this policy could be provided to the subject also after the apprehension of personal data).

This privacy policy (Article 5.6 of the Standard [69]) shall include:

1. the basic information of the data controller (name and address, usual business location, contacts of the person in charge, etc.);

2. the purposes of the collection and use of personal data, as well as the different business functions covered by each purpose;

3. the types of personal data collected by each business function, the collection rules (scope, manner and frequency, storage location, storage time limit);

4. the purposes of sharing, transfer, and public disclosure of data, the types of third-party recipients, and the corresponding legal liabilities;

5. the basic principles followed for data security, the security capabilities, and the measures taken;

6. the data subject rights and mechanisms to use them, such as the method of inquiry, the method of correction, the method of deletion, the method of canceling the account, the method of withdrawing the consent, the method of obtaining a copy of the personal information, the method to restrain automated decision-making, etc.;

[69] Article 5.5 of the revised standard, with minor changes.

7. the potential security risks after the provision of the personal data, and the potential impact of not providing the same data;

8. the channels and mechanism for the data subject inquiry and complaints, as well as external dispute resolution agencies and contact methods.

The revision adds up another information to be included in the privacy policy, regarding the distinction between "core" and "additional" business functions, that we will further examine in the next chapter, and the necessity to highlight if the data processed are sensitive data.

As we have seen, the information that shall be provided by a Chinese entity when collecting data on the ground of consent or via automatic means, are quite similar to the one that shall be provided in any case according to Article 5.6 of the Standard.

Therefore, it is possible, for Chinese data controllers, to provide the same privacy policy whether when the processing is based on consent or made by automatic tools, or when the processing is based on other grounds.

The only substantial difference is that, in the case of a processing based the consent of the data subject or when there is an automatic data collection the Standard requests that the information is given prior to the data collection, while in the case of a processing based on other grounds, the Standard does not explicitly requires that the information is provided before the data collection.

Given this, we can note that many of the information listed by both E.U. and Chinese laws are quite superimposable. When collecting personal data of Chinese citizens in China, then, an E.U. company should then modify its privacy policy with a clear statement about the manner and frequency of the data collection (not requested in the same way by E.U. Law) and with an explanation of its data security capabilities, which E.U. Law states that the data controller shall not disclose with the data subject (except in the case of a data transfer outside E.U.) but shall keep available for authority inspection. An E.U. company should also, when collecting data on the ground of the consent of the data subject, consider that it needs to provide him/her the privacy policy before collecting the data.

When collecting personal data of E.U. citizens in Europe, when offering goods or services in E.U., or when monitoring the behavior of E.U. citizens in Europe, instead, a Chinese company should modify its privacy policy including the list of rights granted to the data subject and set out in Article 13 GDPR, including the right to lodge a complaint with a supervisory authority. Finally, it should acknowledge the existence of automated decision-making (e.g. profiling), and provide meaningful information about the logic involved in the automated decision-making, in order to let the subject understand how the automated mechanism works and could affect his/her data and his/her service.

Also, a Chinese company that collects data under the scope of GDPR, should

evaluate if it needs to appoint a data protection officer according to GDPR rules (and, in the case, give its contact details in the information provided to the data subject). Lastly, a Chinese company, when processing data under GDPR, could take advantage of the chance to process data based on its legitimate interest (giving, in the case, information to the data subject about the legitimate interest pursued).

4.4. The rights of the data subject in China and in the E.U.

As we have seen, both GDPR and the Guobiao requires that the privacy policy lists the rights of the data subject.

The rights enlisted in both laws are quite similar but with some meaningful differences.

As for the GDPR, the rights of the data subject are listed in Articles 15-22 as follows:

– the right of access, according to which the data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data (Article 15);

– the right of rectification, according to which the data subject shall have the right to obtain from the controller without undue delay the rectification of inaccurate personal data concerning him or her (Article 16);

– the right to erasure ("right to be forgotten") according to which the data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay (Article 17);

– the right to obtain from the controller restriction of processing (Article 18);

– the right to portability, according to which the data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided (Article 20);

– the right to object, on grounds relating to his or her particular situation, at any time to processing of personal data concerning him or her (Article 21);

– the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her. (Article 22).

In the Chinese Guobiao, instead, these rights (listed in Article 7 [70]) are as follows:

– the right of access, according to which the data subject shall have the right to obtain from the controller access to personal data concerning him or to the categories of personal data concerning him, as long as to the origin and purpose of use of the data and the identity third parties which have obtained the same data (Article 7.4);

– the right of rectification, according to which when a data subject finds an error or something incomplete about their data held by a data controller, it should provide a way to modify data according to the request of the data subject (Article 7.5);

– the right of erasure, according to which a data controller should promptly delete data if it has violated laws or regulations in the collection or use of data or if it has violated an agreement with the data subject in the collection or use of data (Article 7.6);

– the right to withdraw consent, according to which the data subject should be provided with ways to withdraw authorized consent to collect and use their (Article 7.7);

– the right to cancel an account, according to which data controllers who provide services through registered accounts should provide means for data subjects to cancel their account in a simple and convenient way (Article 7.8);

– the right to obtain copy, according to which data controllers should provide data subjects a way to obtain copies of data regarding "individual basic information" and data regarding health, psychological, education and work information, or if technically feasible, directly transfer them to the third party chosen by the data subject (Article 7.9);

the right to file a complaint in case of automated decision making if it could have a significant impact on the data subject's rights and interests (Article 7.10).

Both the regulations open their lists with the right to access data, but the Chinese Standard does not require that the data controller displays every data it is processing, but only to the "categories" of personal data processed by the data controller.

As for the right to rectification the Chinese and the E.U. definition are quite superimposable, as well as the one regarding the right of appeal in the case of an automatic decision making that could have a significant impact on the data subject's rights and interests, as we have seen in Chapter 3.2.

Moving on to the right to be forgotten, it is quite different in the Chinese

[70] Article 8 in the revised Standard.

Guobiao compared to the one present in GDPR. Article 7.6 [71] of the Guobiao in fact provides that the right of erasure is tied to a violation of law by the data controller.

On the other side, Article 17 of the GDPR states that the right to be forgotten may be exercised also when the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed. This right has been developed after the E.U. Court of Justice has stated, in 2014, that in order to comply with the rights laid down in E.U. regulations the operator of a search engine is obliged: 'to remove from the list of results displayed following a search made on the basis of a person's name, links to web pages, published by third parties and containing information relating to that person, also in a case where that name or information is not erased beforehand or simultaneously from those web pages, and even, as the case may be, when its publication in itself on those pages is lawful'. [72]

The right to be forgotten finds meaning precisely in this case, where the data processing is lawful, but data are no longer necessary in relation to the purposes for which they were collected or otherwise processed.

As for the right to obtain copy, present in the Chinese Standard, this right could be compared to the right to portability granted in GDPR but, while E.U. law states that the data controller shall provide the data subject with his or her data 'in a structured, commonly used and machine-readable format', Chinese law provides instead, more broadly, that the data controller shall transfer personal data directly to the third party chosen by the data subject 'if technically feasible'.

The data portability rule has been criticized in E.U. for its being generic about the formats and for being too difficult to implement. [73] Chinese rule, being more general, has a lesser impact, but on the other side avoids the risks caused by the strict and tricky to implement European rule.

As for the right to withdraw consent, GDPR includes it in Article 13 (that provides the aforementioned list of information that the data controller must provide to the data subject), while the Chinese standard lists it among the rights to be granted to the data subject, but the essence of the rule does not change. It is possible to withdraw consent at any time and both rules specify that the withdrawn of consent does not affect the lawfulness of processing based on consent before its withdrawal.

---

[71] As well Article 8.3 of the revised Standard.

[72] Judgment of 13 May 2014 *Google Spain and Google*, C-131/12, EU:C:2014:317, paragraph 88.

[73] See: J Wong, T Henderson, 'How Portable is Portable? : Exercising the GDPR's Right to Data Portability' (2018) Pervasive and Ubiquitous Computing and Wearable Computers, 911–920.

Likewise, the right to cancel an account is similar in the E.U. an in China and is implicit in the E.U. right to erasure and in the right of restriction. This specific right is a definite sign of the Chinese interest to protect its citizens when they disseminate their own data online.

Lastly, the right to object, on grounds relating to his or her particular situation, at any time to processing of personal data concerning him or her, is present only in the GDPR and not in its Chinese counterpart. This right to object is directly addressed to processing made in the public interest and/or on the basis of legitimate interest.

The absence of the right to object in the Chinese Standard is therefore related from one side to the fact that the Standard is not directed to public bodies, and from the other side to the absence of a lawful processing based on the legitimate interest of the data controller or of a third party.

It will be, anyway, important to add this right when the Standard will discipline also personal data processing made by administrative authorities.

We have, therefore, a complete set of rights provided both in GDPR and in the Chinese Guobiao, that testify to the Chinese choice to tighten its privacy law according to the reference standard.

Only few differences remain, and some of them call for an implementation when China will sediment its privacy and data protection culture.

4.5. The concept of "consent" in China and in the E.U.

Bearing this in mind, we can examine the differences between China and E.U. when dealing with "consent" for the purposes of the law of personal data protection. In China the law does not require explicit and free consent in order to process personal data, but the recommended standard GB/t 35273–2017 prohibits data processing unless a free consent is given. According to the Standard (Article 3.6) the free consent shall be provided by an "affirmative action", which includes a voluntary statement (in electronic or paper form), also via checking a box, or clicking "agree," "sign up," "send," "dial," etc.

The proposed revision both strengthen and weakens this framework.

From one side the revision offers a much-welcomed distinction between "basic business functions" (*jīběn yèwù gōngnéng* 基本业务功能) and "additional business functions" (*kuòzhǎn yèwù gōngnéng* 扩展业务功能). The former is aimed to meet the desiderata of the consumer, in his perspective (e.g. the use of an email address to answer one's email inquiry), the latter is aimed to expand the data processing beyond the expectations of the data subject.

In the revision, Appendix C2, C3 and C4 help identify "basic business func-

tions" and "additional business functions". For example, the improvement of product or services, the enhancement of user experience or the development of new services shall not be classified as basic functions.

When processing data, a data controller should seek consent for the basic business functions and then obtain consent for each and every processing activity that falls under the scope of the "additional business functions".

Before the additional business function is used for the first time, the data controller should inform the data subjects through the interactive interface or design (e.g. via pop-up windows, filling boxes, etc.).

The revision, in this regard makes the Chinese Standard much closer to E.U. rules, which requests "granular" consent collection for the various purposes pursued by the data controller, giving the data subject the chance to freely select if he/she wants to give consent for each purpose presented.

Recital 32 of GDPR indeed states: 'Consent should be given by a clear affirmative act establishing a freely given, specific, informed and unambiguous indication of the data subject's agreement to the processing of personal data relating to him or her, such as by a written statement, including by electronic means, or an oral statement. This could include ticking a box when visiting an internet website, choosing technical settings for information society services or another statement or conduct which clearly indicates in this context the data subject's acceptance of the proposed processing of his or her personal data. Silence, pre-ticked boxes or inactivity should not therefore constitute consent. Consent should cover all processing activities carried out for the same purpose or purposes. When the processing has multiple purposes, consent should be given for all of them. If the data subject's consent is to be given following a request by electronic means, the request must be clear, concise and not unnecessarily disruptive to the use of the service for which it is provided'.

Given this, the Chinese choice seems more rational since it breaks down the consent in the two macro-categories basic and advanced business functions, of which the first is what the data subject expects from the service and the second is whatever the data controller wants to "add up", thus consenting a more efficient way to deal with consent, avoiding unnecessary confusion between mandatory and optional consent.

The European choice, for its part, provides a more complex subdivision of consents, that does not keep into account what the consumer expects from the service provided.

From the other side the revision contained in GB/t 35273-2020 weakens the safeguards for Chinese data subjects with the introduction of the so-called "implicit consent" (in Article 3.7).

This "implicit consent" (shòuquán tóngyì 授权同意) as opposed to the "ex-

press consent" (míngshì tóngyì 明示同意) disciplined in Article 3.6 of the Standard, includes negative actions, such as not leaving a website after being informed of the data processing.

This distinction is surely a step back from the original discipline, intended to reserve for selected categories of data and processing an affirmative consent.

The renewed Guobiao calls for an express consent when the data processing concerns "additional business functions" or whenever it involves sensitive data, biometric information or data related to minors under the age of fourteen.

The affirmative consent is needed also when the identity of the data controller changes as a result of an acquisition, merger, bankruptcy, ecc. and the purpose of data processing varies as well (Article 9.3 lett. b) of the renewed Standard) and, lastly, when the data controller intends to publicly disclose the data.

When comparing E.U. law and Chinese Guobiao, then, another significant difference that arise is the one related to the absence, in the latter, of the legitimate interest. The legitimate interest of the data controller or a third party is not, therefore, a valid legal basis for data processing in China. This "jolly" has proved itself very useful in E.U. in order to loosen a bit the strict terms of the Regulation, letting the data controller to make a comparison between the interests at stake and deem worthy or not the intended processing. [74]

Since the Chinese Guobiao is as strict as the E.U. Regulation in terms of consent, and could be even stricter after its revision will enter into force, it would be probably a good idea to introduce such a "wild card" to use in order to legitimate processing in limited, deserving occasions.

Suffice it to say that in the E.U. the activity of Research and Development of a product sold to a customer could involve the same costumer on the ground of the legitimate interest of the producer to ask him/her to provide feedback on what he/she has purchased. In China, since this activity cannot be classified as a "core activity" of the contract, it could be carried out only with the prior consent of the data subject. [75]

However, disciplining an institute like the one of the legitimate interest, based upon a delicate balancing of interests, makes it absolutely necessary to explain in detail how this works and control that it won't be abused. The easiest way to do so is probably to appoint an independent authority, in charge for giving opinions, control and penalties. The lack of a supervisory authority dedicated to data protection is, therefore, probably one of the major issues of the

[74] I Kamara, P de Hert 'Understanding the balancing act behind the legitimate interest of the controller ground: A pragmatic approach' in E. Selinger, J. Polonetsky, O. Tene (eds.), *Cambridge handbook of consumer privacy* (Cambridge Univ Press 2018) 321-352.

[75] Obviously only if the data controller adheres to the GB/t 35273 Standard.

Standard, since the Cyberspace Administration of China (appointed by the Cybersecurity law as a reference authority) is competent only if the data processing is made using IT tools.

4.6. The Person in Charge of Network Security and the Data Protection Officer: similarities and differences

As we have seen, GB/t 35273–2017 requires the appointment of an in-house responsible for data protection for businesses which meet certain requirements. The responsible for data protection is quite different from the data protection officer covered under E.U. GDPR.

Let's start from the requirements that made the appointment compulsory.

According to the Chinese Standard, the organizations which main business involve the processing of personal data and have more than 200 employees have to appoint a responsible for data protection, as well as the organizations that process data of more than 500.000 people (the revision will raise this threshold to 1.000.000 people) or expect to do so within 12 months shall appoint a responsible for data protection.

E.U. Law requires the appointment of a data protection officer when the processing is carried out by a public authority or body, when the core activities of the controller consist of processing data with regular and systematic monitoring of data subjects on a large scale, and when the core activities of the controller consist of processing on a large scale of special categories of data. The threshold for appointment is similar in both the norms, in the E.U. law the concept of "large scale" (exemplified in many occasions by supervisory authorities [76]) plays a key role.

A partial remedy here will be provided when the revision of the Chinese standard will come into force, offering a new threshold for data controllers that process sensitive data (they will need to appoint a responsible for data protection if process sensitive data of more than 100.000 people). [77] Albeit being too high, this threshold is however comforting, since the absence of a distinction in

[76] E.g. some examples for the healthcare sector were provided by the Dutch Supervisory Authority (AP): https://autoriteitpersoonsgegevens.nl/nl/nieuws/ap-geeft-uitleg-over-grootschalige-gegevensverwerking-de-zorg Last accessed on September 2020. Some useful directions on the "large scale" concept can also be found in the Guidelines on Data Protection Impact Assessment (DPIA) from the Article 29 Working Party (wp248rev.01), last amended on October 13, 2017: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236 Last accessed on September 2020.

[77] Article 10.2 lett. C) (3) of GB/t 35273/2020.

the threshold between "common" data processing and "sensitive" data processing was a serious gap in the Chinese discipline.

Moving to the tasks, the responsible for data protection has the task of coordinate and carry out data protection, to formulate, implement and update a privacy policy, to conduct data protection impact assessments, to enlist the data processing conducted by the business, to organize data protection training, to examine data protection related to new services or products, to conduct security training.

Here the differences with E.U. law are considerable. All the tasks of the responsible are tasks assigned to the data controller and its privacy team. The tasks of the data protection officer (listed in Article 39 of Reg. (EU) 679/2016) are the monitoring of the compliance with data protection law by the controller, to provide advice when requested and to cooperate and act as a contact point with the supervisory authority.

Again, the difference between Chinese and E.U. law arise from the lack of an independent authority to safeguard a healthy application of data protection rules. The same difference can be seen in the discipline of data breach, where to have an independent specialized authority as a "first responder" is surely an opportunity.

4.7. Personal data protection Law and Big Data

The abuse of big data [78] is one of the major concerns for data protection nowadays, as we have seen data protection legislation develops along with worrisome technological developments. Well, the current challenge to face is how to deal with these enormous amounts of data, that could be used in order to profile both large numbers of people or single individuals and could be shared with little if no effort at all.

Both E.U. and Chinese rules adopt a principle of data minimization, that if thoroughly applied could stern the risks connected with the abuse of big data.

E.U. Law provides, at Article 5, that the data processing shall be 'adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation')'.

The Guobiao, for its part, sets this principle in Article 5.2, where it is stated that businesses could process only data that have a direct relationship with the

[78] Big Data have been defined as "data that exceeds the processing capacity of conventional database systems." (Source: M Corrales, M Fenwick, N Forgó, 'Introduction' in M Corrales, M Fenwick, N Forgó (eds.) *New Technology, Big Data and the Law* (Springer Nature 2020) 3.

realization of business purposes. The Standard then is sure to specify that "direct relationship" means that without the personal data, the products or services sold could not be used. The Standard also requires the minimum possible frequency for automatic collection of data and in parallel the collection of only the minimum possible quantity of data.

Despite these rules, as we have seen, Chinese society is still prone to a "socialization" of data, since an intrusive breach in someone personal life is tolerated if it allows to obtain a greater good. In this regard, "human flesh search" is a meaningful phenomenon, eagerly developed in China, where collaborative effort by netizens is set to "hunt down" someone that deserves to be found and, maybe, "shamed". Here, Chinese netizens expect from one side large datasets of personal data readily accessible and from one other side impunity.

Until 2009 this perception was substantiated by the case-law. That year, the Wang Fei v. Zhang Leyi case [79] was decided, with the condemnation of the person that spread personal data of the victim, kicking off the human flesh search. The amount awarded to the victim was, however, very low. According to some commentators [80] the low amount awarded (later confirmed by the Court of Appeal) reflects the indulgence of the Court toward human flesh search behaviors.

Also, Chinese government, in order to attain the greater good of social stability and once sampled the great benefits that a widespread video surveillance system could provide to law enforcement authorities, endorsed an expansion and improvement of the same surveillance system.

In doing so, Chinese government inevitably collects a tremendous amount of data. Also, these data are elaborated with the help of artificial intelligences, thereby increasing even more the invasiveness of the surveillance. Pushing the project forward, many issues related to privacy concerns were raised. [81] Chinese government officials answered these objections highlighting the numerous measures adopted to the protection of personal data involved, and justified the widespread control balancing privacy concerns with personal safety concerns, considering the latter more worthy of protection.

---

[79] The case originated when a friend of the wife of Wang Fei (who had an affair) published the diary of the wife, who commit suicide after discovering the affair. Chinese netizens then exposed other personal data of Wang Fei and his lover, subjecting them to public shaming and verbal assaults.

[80] R Ong, 'Online vigilante justice Chinese style and privacy in China' (2012) 21(2) Information & Communications Technology Law 127-145; Dong Han, 'Search boundaries: human flesh search, privacy law, and internet regulation in China' (2018) 28(4) Asian Journal of Communication 434, 447.

[81] B Aho, R Duffield, 'Beyond surveillance capitalism: Privacy, regulation and big data in Europe and China (2020) 49:2 Economy and Society.

The real Chinese policy regarding big data is therefore contained not in the GB/t Standard, but rather in the Social Credit System Project, in the Skynet Project and in the Smart City Project. [82]

While E.U. tries to curb personal data accumulation, China tries to centralize them in the hand of the Government, taking at a level previously unimaginable the so-called "surveillance capitalism" [83]. In this regard the fragile recommended Standard GB/t 5273–2017 pales in the face of the efforts made by the Chinese Government to trace the activities of its citizens.

Not even Article 1039 of China's Civil Code (which will enter into force in 2021) will be able to limit this activities, since when it disciplines data processing by administrative bodies it simply states that those shall keep confidential the personal information of natural persons known in the course of performing their duties, and shall not disclose or illegally provide them to others, but implicitly consent such activities of data gathering to be performed far over the limits set by the principle of data minimization.

What differs in E.U. and China is, as said, the balance of interests between social safety and national interests from one side and privacy and personal data protection from the other side. While China has chosen the former, E.U. has focused on the latter.

A question remains, which is the best balance of interest in the case?

While Europe sacrifice on the altar of data protection a perfect chance to empower its law enforcement, China takes full advantage of the possibilities offered by modern technology, at the price of total surveillance.

5. Conclusions

As we have seen a concept of privacy "with Chinese characteristics" was rooted in China for a long time. [84] This concept of privacy was willing to sacrifice to a certain extent the right to self-isolate in order to guarantee social harmony.

Nowadays, a piece of that concept still lives, shaping what privacy is in China and justifying a path that differs from the Western one on the subject. While the whole world sets toward a concept of privacy shared in its core tenets, it is clear that some secondary (but nevertheless not irrelevant) aspects of personal

[82] ibid.

[83] S Zuboff 'Big Other: Surveillance capitalism and the prospects of an information civilization' (2015) 30(1) Journal of Information Technology 75–89.

[84] See n. 32, 33.

data protection rules take different shapes according to the different jurisdictions examined.

Even with a Regulation and a Standard that look so much alike (and bear witness to this evolution based on a worldwide trend), in actual fact China and E.U. apply personal data protection in different ways.

The core principles of privacy and data protection (that extend throughout the whole world) can be seen in this comparison with the overlap of many dispositions from the E.U. legislation and the Chinese one. The focus on the consent of the data subject [85], the right to be informed, the safeguard measures for personal data security, and the same definition of personal data are appear, in fact, very similar when confronting the latest innovation in privacy law both in China and in the E.U.

This is thanks to the latest effort of the Chinese legislator, that has developed in a short period of time, a comprehensive legislation in the privacy field, in step with the well-established E.U. Law. Suffice to say that, in some respects, Chinese legislation seems stricter [86] (since it requests that privacy policies are provided to the data subject before the data collection) or better drafted (in its distinction between basic and advanced business functions) than its European counterpart.

The analysis highlights that the worries related to the technological sector are a major drive in the Chinese Standard (e.g. in the separate right to cancel an account, and in the various "notes" that exemplifies rules to fit in the informatic environment), while the economic drive plays a major role in the E.U. Regulation (marked by its impressive set of sanctions).

The long and stratified history of privacy and data protection measures in E.U. plays a role in its law, that fits in a society well aware of the values of personal data protection.

China, on the other side, has developed at an increasing pace in the privacy field, therefore its social fabric (and its government) is not fully prepared to adopt a standard as rigid as the E.U. one. For this reason, the Chinese government has put in place the Guobiao GB/t 35273–2017 as a practice run, in order to accustom its businesses to an increasingly strict ruling in the field.

The second step in this direction is the crystallization of the core principles of privacy and personal information protection in the Civil Code and the finalizing move will be the enactment of a personal data protection law by the end of 2022.

---

[85] Although watered-down in the revision that will be applicable from 01 October 2020.

[86] Albeit it is contained in a merely recommended standard. We should in fact remember that this same standard, by virtue of the peculiar temper of Chinese legal system, is less "optional" than it appears to be for many players. Also this same standard will be the basis for future binding legislation in the field.

5.1. Personal Data Protection Law as a tool to rule a global phenomenon

As we said, perhaps the most interesting result of this comparison is the highlight that China and E.U. have developed comparable rules and share a common approach on privacy and personal data protection.

As said, the most prominent endeavour of the Chinese legislator is related to the demands of the technological sector, a drive that is clearly demonstrated by the introduction of specialized courts to deal with tech related cases (i.e. Internet Courts).

Despite the seen differences, in fact, in a globalized world the IT field needs common rules, so then China has tried to implement a state-of-the-art personal data protection for technology users (both Chinese citizens and foreigners that use Chinese technology).

These efforts resulted in the Cybersecurity Law and in the Standard GB/t 35273-2017. This complex work surely paid off as to the form, with a set of rules that provides rigid terms and clear requirements for data processing.

As global phenomena, privacy and data protection need universal rules, because these are supposed to rule data, a volatile asset that can be managed everywhere in the world, regardless of the nationality of the data subject.

So it is a forward-looking choice for China to harmonize its laws to the reference standard (GDPR) in order to ease for its companies to adapt their policies, networks and security measures in order to process data of Chinese citizens as well as of people from the rest of the world.

This also means that privacy in China is no more a second-tier right and that the People's Republic will soon enough require compliance to strict standards from businesses that would like to process data of Chinese citizens.

But we should also consider that privacy and personal data protection will never be the same in China and in the E.U., given the value of the traditional formant in the People's Republic, that values privacy in a way that is quite different that in the West.

A clear demonstration of this difference lies in the phenomenon of the human flesh search [87], that is, still today, carried out with unparalleled extension in China than in other countries, that bears witness to the willingness of Chinese citizens to sacrifice a fraction of each citizen in order to obtain safety and, eventually, harmony.

Also, the fact that Chinese citizens often welcome a widespread dissemination of video surveillance cameras [88] explains much about the different approach toward privacy in China compared with E.U.

---

[87] See n. 62.

[88] See: H Zhang, J Guo, C Deng, Y Fan, F Gu, 'Can Video Surveillance Systems Promote the

The Chinese government seems then to grant privacy to its citizens only when dealing with companies, but not when dealing with the government itself.

So, the question that arise is why Chinese government adopted a Standard so similar to its European counterpart. The answer is probably that both GDPR and GB/t 35273–2017 are tools, that can vary in their effectiveness depending on the values prioritised in the country examined, and on the consequent balancing of interest between privacy and other values.

For example Article 5.4 of the Chinese Standard [89] sets that a data controller does not need to obtain consent from the data subject for the processing of data under a series of situations (e.g. when data are directly related to public safety, public health, or significant public interests, criminal investigation, prosecution, trial, judgment enforcement, or when the data processing is aimed to safeguard major lawful rights and interests).

On the same page the GDPR states (in Article 6), that a data controller does not need to obtain consent from the data subject for the processing of data under a comparable set of situations (e.g. when the data processing is made in compliance with a legal obligation, when processing is necessary in order to protect the vital interests of the data subject or of another natural person, when processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller and, lastly, when processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party).

Therefore, both rules can perfectly fit to various different countries and legal traditions and can vary along with the spirit of the time. The law is the same, the difference is in the interests balancing.

5.2. The challenges on the horizon

This does not mean that China has already overcame every difficulty.

What still lacks in China is, obviously and first of all, a binding rule to take over for the recommended standard GB/t 35273/2017 (the soft power of politics in China that can make substantially binding an optional standard, if endorsed at the political level is surely not enough on the long run) and an independent supervisory authority, that could take the lead in set in the relevant context the rules of the Standard. Chinese laws are still fragmented and focused on various

Perception of Safety? Evidence from Surveys on Residents in Beijing, China' (2019) 11(6) Sustainability MDPI 1,21.

[89] Article 5.6 of the of the revised Standard GB/t 35273/2020.

different aspects of privacy and personal data protection, this led to the creation of various authorities (e.g. the Cyberspace Administration of China, which is the authority supervising the application of the Cybersecurity Law, but cannot be involved when a data breach happens "offline").

It will be important also to revise the right to be forgotten, which is now tied to a violation of law by the data controller according to Article 7.6 of the Chinese Standard, while the E.U. rule states (Article 17) that the right to erasure may be invoked simply when the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed.

Another thing that should be implemented as soon as possible is a set of sanctions to measure for tech giants. In practice, the most significant innovation introduced with the GDPR in Europe is the renewed set of sanctions, more proportional but able to frighten multinational corporations, this still lacks in China.

It will be important also that China will implement privacy with the same pace and rules both for private businesses and for State administrations, because the fact that the Standard 35273–2017 (merely recommended) appears applicable only to private enterprises legitimate us to expect that even when it will be transferred in a binding standard it will set aside public administrations, and this could be very problematic.

Again, we are dealing with a tool, that can be more or less effective according to the balancing of interests adopted, this fact suggests to choose at least a formal implementation of personal data protection for every data controller, thus granting a common framework and guarantees to every data subject, without standing in the way when more important right to safeguard are at stake (but hoping that, over time, it could adapt to a situation where privacy and personal data protection are more relevant in the citizen-government relationship in China).

Even if Chinese government will impose compliance with GB/t 35273-2017 to its public bodies, they would still be able to protect the safety of the country and of Chinese citizens, processing data via one of the seen exceptions provided in Article 5.4 of the Guobiao (e.g. Art. 5.4 letter b), that consent data processing without consent if the data are 'directly related to public safety, public health, and significant public interests', or letter c), that consent data processing without consent if the data are 'directly related to criminal investigation, prosecution, trial, and judgment enforcement, etc.' or even letter d), that consent data processing 'when safeguarding major lawful rights and interests').

The other differences that arose in the comparison refer to mere choice of details, that do not undermine the framework of Chinese personal information protection law.

As said the next step, for China, is therefore to make GB/t 35273–2017

mandatory in order to instil greater awareness of the privacy issue to its companies, its authorities and its citizens. Doing so, China could help to shape a global personal data protection law, since every country can agree on some common principles in this field, leaving to each individual nation the choice of balancing between privacy and other core values of its society.

In this regard, the revision of the Standard, recently adopted (on 06 March 2020) has dampened enthusiasm to some extent with its entry into force set far away in October 2020 and with its step down on consent (caused by the introduction of the so-called "implicit consent") despite bringing up some positive news and trims to the Standard.

Again, the real bone of contention could be the field of big data where, as we have seen, the interest of the Government, as well of the private sector, and as well of the citizens goes in the direction of an increased tolerance in order to process these personal data to pursue other relevant values. Both in China and in the E.U. this push leads to a balancing of interests, that today tends more toward social justice or social harmony in China compared to what happens in Europe.

This does not mean that it is impossible to implement a full-fledged culture of privacy, where citizens and businesses value data protection, in China, despite the fact that the society still tolerates an impairment of privacy in order to attain social justice or social harmony.

If this "impairment" is justified with a reasonable balancing of interests and presided by strong security measures granting a safe and controlled data processing, then it could become a central pillar of a Chinese privacy culture.

As always when it comes to China, there is no wrong or right, only time will tell whether it's better to live without social interference, but feeling less safe, or to feel safer, but with overseeing.