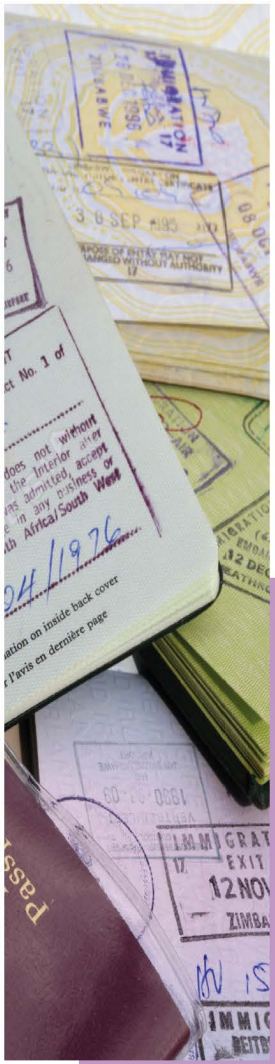
European Parliament

DIRECTORATE-GENERAL FOR INTERNAL POLICIES

POLICY DEPARTMENT C
CITIZENS' RIGHTS AND CONSTITUTIONAL AFFAIRS



Constitutional Affairs

Justice, Freedom and Security

Gender Equality

Legal and Parliamentary Affairs

Petitions

The data protection regime in China

In-depth Analysis for the LIBE Committee

EN

2015

DIRECTORATE GENERAL FOR INTERNAL POLICIES

POLICY DEPARTMENT C: CITIZENS' RIGHTS AND CONSTITUTIONAL AFFAIRS

CIVIL LIBERTIES, JUSTICE AND HOME AFFAIRS

The data protection regime in China

IN-DEPTH ANALYSIS

Abstract

This in-depth analysis was commissioned by the European Parliament's Policy Department for Citizens' Rights and Constitutional Affairs at the request of the LIBE Committee.

One cannot talk of a proper data protection regime in China, at least not as it is perceived in the EU. The international data protection fundamentals that may be derived from all relevant regulatory instruments in force today, namely the personal data processing principles and the individual rights to information, access and rectification, are not unequivocally granted under Chinese law. An efficient enforcement mechanism, also required under European standards, is equally not provided for. China has no comprehensive data protection act but several relevant sectorial laws that, under a combined reading together with basic criminal and civil law provisions, may add up to a data protection 'cumulative effect'. This assertion is examined and assessed in the analysis that follows. A list of realistic policy recommendations has been drawn up in order to establish whether China's recent data protection effort is part of a persistent, yet concise, policy.

DOCUMENT REQUESTED BY THE
COMMITTEE ON CIVIL LIBERTIES, JUSTICE AND HOME AFFAIRS (LIBE)

AUTHORS

Prof. Paul de Hert, Vrije Universiteit Brussel, VUB

Dr. Vagelis Papakonstantinou, Vrije Universiteit Brussel, VUB

RESPONSIBLE ADMINISTRATOR

Mr Alessandro DAVOLI
Policy Department C - Citizens' Rights and Constitutional Affairs
European Parliament
B-1047 Brussels
E-mail: poldep-citizens@europarl.europa.eu

LINGUISTIC VERSIONS

Original: EN

ABOUT THE EDITOR

Policy Departments provide in-house and external expertise to support EP committees and other parliamentary bodies in shaping legislation and exercising democratic scrutiny.

To contact the Policy Department or to subscribe to its monthly newsletter please write to:
poldep-citizens@europarl.europa.eu

European Parliament, manuscript completed in October 2015.

This document is available on the Internet at:
http://www.europarl.europa.eu/studies

DISCLAIMER

CONTENTS

EXECUTIVE SUMMARY

The assessment of a Western-type human rights model against an Asian background is by no means an easy task, given the **big differences in the cultures** involved. This task is further burdened when the country in question is China, where the **essential human rights' conditions (horizontal application, independent courts and legal certainty) are not in place**. However, the fact that China constitutes today a central economic power, a **major EU trade partner** and a substantial global political player means that **realism is advisable** when it comes to comparative law exercises.

On the other hand, the EU is still an international data protection laboratory, even if it is an advanced one. Apart from giving birth to the first relevant legislative texts, its Member States have applied data protection legislation vigorously and consistently over the past 40 years, some of them having already reached their second or third generation of data protection acts. At EU level the **1995 Data Protection Directive**, still in effect today, has solidified the EU data protection model, that was subsequently exported to third countries as well. Recently, new rights and ideas that are included in its **draft General Data Protection Regulation, currently under elaboration**, have already raised debates across the globe. Once finalised, it is expected to raise the EU data protection threshold even higher. Nevertheless, although the majority of countries around the globe have implemented data protection laws within their jurisdictions, until today no global standard exists, the EU model most likely occupying the global reference position but not that of the global standard applicable. The above distinction serves to warn those accustomed to the EU model that, when stepping outside the EU, they have to be aware that, first, the EU is not the preferred international data protection model for the time being and, second, the terms "data protection", "information privacy" or "data privacy" may have a different meaning to that of the EU.

One cannot talk of a proper data protection regime in China, at least not as it is perceived in the EU. What is decisively different between China and the EU is their underlying approach to personal data processing. Even if one chooses to disregard the **human rights parameter** for the sake of the analysis, the fact remains that **whatever data protection** exists **in China today,** it is **aimed exclusively at the individual as consumer**. The data protection recipient is **not an individual or a "data subject", as in the EU**, but a consumer. However, the protection of the right to privacy may fare far better under current Chinese law. The **right to privacy** - where however "privacy" is perceived differently in China than in Europe - is enshrined in basic Chinese law, ultimately connected to the **right to dignity**. Although the distinction between the two rights is by now clear in EU law, for the purposes of this analysis and in order to achieve a comprehensive approach, the concept of privacy protection will also be elaborated under the "data protection regime" title.

China does **not** have **a general data protection act** but traces of data protection may be found in a **multitude of sector-specific legal instruments**. Notwithstanding the issues of **democracy and the rule of law**, data protection provisions may be found in its **Criminal and Civil law** as well as in a **number of instruments released by** China's second-highest legislative organ, **the Standing Committee of its National People's Congress** (SC-NPC) and by the Chinese **Ministry of Industry and Information Technology** (MIIT). In fact, the SC-NPC 2012 Decision constitutes the *de facto* data protection standard in China today. **A combined reading of all these provisions leads to a suggestion of a "*cumulative effect*" that characterizes the Chinese approach to data protection today**. However, data protection is a system that cannot, and should not, be broken down into its constitutional parts in order to be able to construct a comparison and derive com-

mon ground. This system is evidenced by the common ideas found in **all relevant international instruments in effect today**: the EU 1995 Data Protection Directive, the Council of Europe Data Protection Convention, the OECD Guidelines and the APEC Privacy Framework. They all include a set of **basic data processing principles** (the fair information principles) and a set of basic data protection rights (information, access, rectification). Europeans would also add an efficient enforcement mechanism to that list. It is not possible to break this system down into its components, because one does not function without the others. In this context, it is established in this report that **the basics of international data protection are not unequivocally in place in China today**.

If a legalistic approach was adopted, then no common ground could be found between two fundamentally different systems both in their wording and in their *raison d'être*. Consequently, **data transfers would need to be prohibited towards China, on the basis of Article 25 of the EU 1995 Data Protection Directive**. However, **this would be an impractical**, if not unnecessary position. Over the past few years China has **enacted a series of data protection-related legal texts**; this **initiative** need not be discouraged but **rather strengthened** and tested, particularly given the fact that personal data flows between the EU and China might become a pressing reality within **contemporary cloud computing environments**, where vast data centres may be installed (or are already operating) in China. We therefore believe that, while **commercial and other relationships** need not be stifled on data protection grounds, **concrete and specific policy recommendations need to be provided to China**. Thus, China would have the opportunity to demonstrate that its **recent data protection effort** is **part of** a **persistent, yet concise, policy** and not just a pretext to attract more internal and external information processing business. To this end a **list of policy recommendations** has been drawn up with regard to (a) the basic **data protection principles**, (b) the basic data protection **individual rights**, (c) **data transfers**, and (d) the **enforcement mechanism**.

INTRODUCTION

KEY FINDINGS

- The assessment of a Western-type human rights model against an Asian background is by no means an easy task, given the big differences in the cultures involved. This task is further burdened when the country in question is China, where the essential human rights' conditions (horizontal application, independent courts and legal certainty) are not in place.
- A careful and flexible approach is advised in order to bring together in a meaningful and practical way two fundamentally different approaches on the issue of human rights that are necessitated by financial and political considerations but are not, in the same way, enabled either by social or by legal factors.
- On the other hand, the individual right to data protection is a relatively recent addition to the EU list of human rights, that is currently furthered through ongoing elaboration of the EU data protection reform package; in particular, the EU General Data Protection Regulation, once in effect, is expected to set the EU data protection threshold even higher.
- Outside the EU, despite of the fact that the majority of countries regulate by now personal data processing, the EU data protection model is not the international standard. In addition, the term "data protection" may have a different meaning to that given within the EU even in countries that have chosen to enact data protection acts within their respective jurisdictions.

The assessment of a Western-type human rights model against an Asian background is by no means an easy task, given the big differences in the cultures involved. This task is further burdened when the country in question is the People's Republic of China (PRC, henceforth China)[1]. Undoubtedly China presents a set of unique characteristics that make such an analysis extremely difficult and subjective, if not impossible. Obviously, the first issue that comes to mind pertains to its political regime. China is an authoritarian state, in stark and at times pointed contrast to western-type democracies. While this difference in political regime may not prohibit commercial or other financial relationships, provided that each party is careful to accommodate the other's particular needs and sensitivities, such approximation is most likely impossible when it comes to the protection of human rights. Human rights were first developed in Europe and thereafter furthered in other parts of the world as well, essentially however upon a democratic background. They are absolute, meaning that they are protected against anyone regardless whether in the private or the public sector, and they need independent courts and legal certainty in order to thrive. All these conditions (horizontal application, independent courts and legal certainty) are not warranted in China today. In fact, the case appears to be quite the opposite, with discussion on human rights allegedly being prohibited in China's higher education and on the internet[2].

[1] See the Preface in Gao Q/Zhang W/Tian F, *The Road to the Rule of Law in Modern China*, Springer, 2015.
[2] Bartow A, *Privacy Laws and Privacy Levers: Online Surveillance versus Economic Development in the People's Republic of China*, 74 OHIO ST. L.J. 853 (2013), see also the blogging censorship case by the Chinese Government against Zhao Jing (pseudonym Michael Anti), when Microsoft was forced to removing words like "democracy" and "human rights", as proved in relevant US Congressional Hearings (Lee J-A, *Regulating Blogging and Microblogging in China*, Oregon Law Review, Vol. 91, No. 2, 2012).

Further characteristics that make the case of China unique refer to its contemporary economic and political power as well as to its chosen model of economic development. The fact that China constitutes today a central economic power, a major EU trade partner and a substantial global political player means that realism is advisable when it comes to comparative law exercises. In the data protection context this would mean, for instance, that a general prohibition of all personal data flows between the EU and China, on the basis of the "*adequacy*" criterion of basic EU data protection law[3], would probably be impractical; however, as the case of the USA has taught us, this is by no means an unprecedented situation for the EU.

The second unique characteristic that China presents refers to its chosen model of economic development: by designating specific regions to specific economic activities and awarding them with the relevant legal status to achieve their purposes, China has developed a complex, multi-layered legal system that needs to be approached on a region-specific level if any meaningful legal analysis is to be achieved. Nevertheless, this task is not only impossible for, and probably useless to, foreigners but also irrelevant when it comes to the protection of human rights, that needs to run through all of the country and not be region-specific. Finally, the multi-level legal structure of China itself, that despite its terminology (e.g. Constitution) is not directly comparable to western-type legal architectures, further adds to the complexity of the task at hand.

If to the above are added the different cultures and histories of the peoples concerned, that at times give different meaning to the same basic notions in the human rights list, the difficulty of the task is made evident. Consequently, **a careful and flexible approach is advised in order to bring together in a meaningful and practical way two fundamentally different approaches on the issue of human rights, that are necessitated by financial and political considerations but are not, in the same way, enabled either by social or by legal factors**.

On the other hand, the individual right to data protection is a recent addition to the EU list of human rights. Despite of the fact that the first data protection acts appeared in Europe some forty years ago and a relevant directive was introduced in 1995, an independent right to data protection, separate from a right to privacy, was entered in the EU constitutional texts only in 2009 with the ratification of the Treaty of Lisbon. The right to data protection, as appearing in the text of Article 16 TFEU, is a "technical" right: although principle-driven, it requires auxiliary legislation to make its principles and requirements concrete in personal data processing instances. In addition, it is exactly the ratification of the Treaty of Lisbon that made an overhaul of the existing EU data protection legal edifice necessary: although the details of the EU data protection reform package, that is still under discussion, need not be analysed within the scope of this analysis, the general idea is that, apart from an updating of outdated provisions, new rights and notions are bound to emerge from this process, such as the right to be forgotten, the right to data portability, privacy by design, data breach notifications or data protection impact assessments. **These additions are expected to set the EU data protection threshold even higher**.

It ought to be noted, however, that all of the above constitute the EU approach to data protection. If viewed from a global perspective, although the majority of countries across the world have chosen to enact national data protection acts within their respective jurisdictions, the EU model remains by far the most strict (and perhaps bureaucratic) among all

[3] Article 25 of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 281, 23.11.1995, p. 31–50 ("1995 Data Protection Directive").

international implementations. Among these countries that by now have national data protection regulations, only the EU member states apply the EU data protection model together with the (altogether 10) countries that have succeeded in being awarded with an "*adequacy*" finding by the EU. A number of other, mostly European, countries have chosen to abide by the, marginally more flexible, Council of Europe data protection model[4], which is also currently under amendment. All other countries around the globe follow their own data protection way. Until today **no global standard exists**, the EU model most likely occupying the global reference position but not that of the global standard applicable. The above distinction **serves at warning those being accustomed to the EU model that, when stepping outside the EU, they have to be aware that, first, the EU is not the preferred international data protection model for the time being and, second, the terms "data protection" (or, even, its equivalents, "information privacy" or "data privacy") may have a different meaning to that of the EU even in countries that have chosen to enact data protection acts within their respective jurisdictions**.

This report purports to elaborate upon the data protection regime in China under the above constraints. To this end after a brief presentation of the EU data protection model under chapter 1, its chapter 2 will be aimed at describing the Chinese data protection regime in effect today. Subsequently, an assessment of its merits and shortcomings will be attempted in chapter 3, before a number of policy recommendations is undertaken in chapter 4. **The authors believe that despite the big differences and apparent incompatibility between the two approaches on data protection, there is space for case-specific sensible solutions that will achieve at least to bridge the perceived gap – if not approximate the two diverging perspectives**.

[4] Primarily based on the Council's Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, 28.1.1981.

1. THE EU DATA PROTECTION MODEL: A PRINCIPLES-DRIVEN SYSTEM FOR THE PROTECTION OF A FUNDAMENTAL HUMAN RIGHT

KEY FINDINGS

- The EU has been, and still is, the international data protection laboratory. New rights and ideas included in its draft General Data Protection Regulation have already raised debates across the globe.
- If the EU data protection model was to be described in a concise manner, it could probably be summed up as a principles-driven system.
- The high-level EU data protection principles are the principles of lawfulness of the processing, access to justice, transparency and accountability.
- The above high-level principles are implemented through a standard set of regulatory mechanisms. These include a list of basic notions and definitions, an enforcement mechanism, a set of individual rights, and a model for data transfers.
- Other international data protection regulatory alternatives are also to be found, that may, or may not, resemble the model followed by Chinese legislators in the field. These include the Council of Europe Data Protection Convention, the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, as well as to the APEC Privacy Framework.

The EU has been, and still is, the international data protection laboratory. Apart from giving birth to the first relevant legislative texts, its Member States have applied data protection legislation at national level vigorously and consistently over the past 40 years, some of them having already reached their second or third generation of data protection acts. At EU level the 1995 Data Protection Directive, still in effect today, has solidified the EU data protection model, that was subsequently exported in third countries as well. The post-9/11 era opened up a thoughtful discussion in the EU as to the acceptable balancing between national security and personal data protection. Today, the draft General Data Protection Regulation[5], still under elaboration, has already sparked an international debate on new rights (the right to be forgotten, the right to data portability), new risk assessment methods (impact assessments in the data protection field), new system design requirements (privacy by design), as well as on the most effective approach to data protection in cloud computing or in the biometrics field. All of the above are the result of decades-long painstaking implementation across the EU, that includes daily challenges in front of courts of all levels and Member State data protection authorities, academic teaching, scholarly writing, as well as active politics.

If the EU data protection model was to be described in a concise manner, it could probably be summed up as a principles-driven system that is implemented through a standard set of regulatory mechanisms. The high-level EU data protection principles are the principles of **lawfulness of the processing, access to justice, transparency and accountability**. The principle of lawfulness of the processing means that personal data processing needs to have a solid legal starting point (consent or a legal mandate or any other recognised or legitimate starting point) as well as a certain quality (fair-

[5] European Commission, *Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)*, COM(2012) 11 final.

ness and lawfulness of the processing, purpose and time specificity, data minimization, security and confidentiality). The principle of access to justice grants individuals effective, timely and accessible means of judicial redress. Under the principle of transparency, all personal data processing, including decision-making by data controllers and data protection authorities, needs to be open and accessible to the public. Finally, the principle of accountability places upon data controllers the burden of implementing within their organizations specific measures in order to ensure that data protection requirements are met. These high-level principles are present both in the 1995 Data Protection Directive and in the current draft of the General Data Protection Regulation.

The above high-level principles are implemented through a standard set of regulatory mechanisms. These include **a list of basic notions and definitions, an enforcement mechanism, a set of individual rights, and a model for data transfers**. The list of basic notions and definitions is central to the EU data protection model: the definitions given to such terms as "personal information", "data subject", "data controller", "filing system" or "processing" run through all EU law and set the necessary basis for discussion. Of equal importance is the enforcement mechanism: an independent state agency, the data protection authority, is dedicated to serving the data protection purposes within the jurisdiction concerned. The data protection-specific individual rights of information, access, objection and rectification warrant individuals with the means to control data flows on them. Finally, the "*adequacy*" model for data transfers, although cumbersome or even outdated in the internet age, ensures that EU data protection legislation will not be circumvented through "data havens" or other similar overseas constructions.

All of the above, meaning high-level principles and accompanying enforcement mechanisms, constitute the EU data protection model. As discussed, outside the EU it is viewed as a strict and perhaps stifling to innovation regulatory model, that it is appreciated only by the handful of countries that have been granted "*adequacy*" finding by the EU. Other data protection lists, in order to test whether data protection legislation is in effect within a given jurisdiction, have also been compiled[6], and it is by their count that international data protection is on the rise with more than one hundred countries adhering to it in one way or another[7]. Evidently, their level of protection differs. If a strict approach was to be adopted, the "data protection" title ought only be awarded to EU Member States and countries with "*adequacy*" finding. Accordingly, as per basic EU data protection law[8], data flows ought to be allowed only among these countries. Nevertheless, this would have been a limiting approach. Apart from punishing countries that are struggling and experimenting on the, essentially new, data protection field, it would also carry serious financial consequences for all the parties involved. This has been acknowledged also by the EU, that has constructed a series of regulatory alternatives for international data flows to indeed take place without abandoning its basic data protection, *adequacy*, approach: these include binding corporate rules, model clauses, as well as, country-specific solutions (the latter pertaining only to the USA and the "safe harbor" arrangement). Consequently, **until today the EU has succeeded in maintaining and furthering its own data protection model, while at the same time acknowledging its not fit-for-all character. The EU has granted to those**

[6] See for instance Greenleaf G, *Asian Data Privacy Laws: Trade & Human Rights Perspectives*, Oxford University Press, 2014, "*for the purposes of this book a country is considered to have a data privacy law only if it has a national law which provides, in relation to most aspects of the operation of the private sector, or its national public sector, or both, a set of basic data privacy principles, to a standard at least including most of the OECD Guidelines or Council of Europe Convention, plus some methods of statutorily mandated enforcement (i.e. not only self-regulation)*" (p.14).
[7] Greenleaf G, *Global data privacy laws 2015: 109 countries, with European laws now a minority*, 133 Privacy Laws & Business International Report, February 2015.
[8] Article 25 of the 1995 Data Protection Directive.

countries interested to cooperate the necessary means to overcome difficulties in a mutually acceptable way, in order to allow personal data flows outside its borders and at the same time not lessen the level of protection afforded to EU data subjects.

1.1. Other international data protection regulatory alternatives: the Council of Europe Data Protection Convention, the OECD Guidelines and the APEC Privacy Framework

Because the EU data protection level is probably unattainable by China, given its regulatory framework currently in effect, as it will be demonstrated in the analysis that immediately follows, reference will be made in this report to other international data protection regulatory alternatives that may, or may not, resemble the model followed by Chinese legislators in the field. In this context, a brief mention needs to be made to the Council of Europe Data Protection Convention, the OECD Guidelines, as well as to the APEC (Asia-Pacific Economic Cooperation) Privacy Framework.

The Council of Europe Data Protection Convention, currently also under review, was signed in 1981, it therefore preceded the EU Data Protection Directive by more than a decade. Despite its age, the Convention remains still relevant because it includes in its provisions all the basic characteristics of the EU data protection model (high-level principles and accompanying enforcement mechanisms), it applies to all processing (including security processing by the state) and, through its protocol, regulated transborder data flows. A significant characteristic is that it is open to ratification for non-European countries as well, an option that has benefited quite a few countries until today.

The OECD Guidelines, currently in their 2013 version[9], broadly follow the EU model of principles and enforcement mechanism but because they are voluntary and more flexible in their wording they have acquired global appeal.

Finally, the APEC Privacy Framework is a voluntary, basic set of rules for personal data processing that, while broadly following the EU structure, greatly differs in terms of enforceability and, ultimately, level of protection afforded to individuals.

[9] OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, 2013.

2. THE DATA PROTECTION REGIME IN CHINA

KEY FINDINGS

- One cannot talk of a proper data protection regime in China, at least not as it is perceived in the EU. What is decisively different between China and the EU is their underlying approach to personal data processing. Even if one chooses to disregard the human rights parameter for the sake of the analysis, the fact remains that whatever data protection exists in China today it is aimed exclusively at the individual as consumer. The data protection recipient is not an individual or a "data subject", as in the EU, but a consumer.
- China does not have a general data protection act but traces of data protection may be found in a multitude of sector-specific legal instruments. A combined reading of all these provisions would suggest a "*cumulative effect*" that is typical of the Chinese approach to data protection today.
- Even outside the EU, data protection is a system that cannot, and should not, be broken down to its constitutional parts in order to be able to draw a comparison and derive common grounds. This system is evidenced by the common ideas found in all relevant international instruments in effect today: the EU 1995 Data Protection Directive, the Council of Europe Data Protection Convention, the OECD Guidelines and the APEC Privacy Framework. They all include a set of basic data processing principles (the fair information principles) and a set of basic data protection rights (information, access, and rectification). It is not possible to break this system down into its components, because one does not function without the others.
- The protection of the right to privacy may fare far better under current Chinese law. The right to privacy, where however "privacy" is perceived differently in China than in Europe, is enshrined in basic Chinese law, both at constitutional and civil law level, ultimately connected to the right to dignity.
- Notwithstanding the issue of democracy and the rule of law in China, data protection provisions (which nonetheless should not be perceived as adding up to a system or a regime) may be found in its Criminal and Civil law, as well as in a number of instruments released by China's second-highest legislative organ, the Standing Committee of its National People's Congress (SC-NPC), as well as by the Chinese Ministry of Industry and Information Technology (MIIT).
- The SC-NPC 2012 Decision constitutes the *de facto* data protection standard. Through combined reading, it regulates all personal data processing undertaken by the private sector in China today.
- The preferred way of individual redress in China to-date are the Criminal and Civil Law provisions, that however have been used until today mostly in cases of identity theft or defamation – and only once, against a foreign subsidiary, for unlawful personal data processing.

While it would have been a legitimate and justified expectation to first define in this report what is meant by "data protection", regardless whether close or far from the EU data protection model, in order then to present and assess the Chinese data protection regime against this definition, we have chosen not to do so, simply because of the fact that **China has no data protection regime**. This finding is based not only on the analysis of the legal provisions actually in effect today, that follows, but also taking account the current underlying approach to personal data processing in China. With regard to its legal regime,

China may not have a general data protection act but traces of data protection may be found in a multitude of sector-specific legal instruments that will be presented below. Because such a sectorial approach is not unique (the case of the USA quickly springs to mind in this regard), one could talk of a **"cumulative effect" that characterizes the Chinese approach to data protection**. While we pay attention to this statement, and attempt to substantiate it in the analysis that follows, we believe that **what is decisively different between China and the EU is their underlying approach to personal data processing**. Even if one chooses to disregard the human rights parameter for the sake of the analysis, the fact remains that **whatever data protection exists in China today it is aimed exclusively at the individual as consumer**. The basic, underlying concept is that data protection is "*instrumentally necessary for the development of e-commerce*"[10]. The data protection recipient is not an individual or a "data subject", as in the EU, but a consumer. In this context, the fact, for instance, that "*every corner of Beijing is now observable on the government's surveillance camera network*" without any word whatsoever on data protection is celebrated as a "*triumph*" by the Chinese police[11]. Accordingly, data protection provisions are not aimed at providing self-determination or even control over an individual's personal information but are rather intended to foster public trust and boost sales. However, this approach is incompatible to that of the EU (or, for the same purposes, any other) data protection law and rather belongs to the consumer law realm. We have established that this is the case for the majority of the Chinese legal instruments allegedly formulating the Chinese data protection regime that are analysed below.

In the same context, it ought to be kept in mind that **data protection is a system that cannot, and should not, be broken down to its constitutional parts in order to be able to construct a comparison and derive common grounds**. The data protection system, even if one moves away from the strict EU data protection model, is evidenced by the common ideas found in all relevant international instruments in place today: the EU 1995 Data Protection Directive, the Council of Europe Data Protection Convention, the OECD Guidelines and the APEC Privacy Framework. They all include a set of basic data processing principles (the fair information principles) and a set of basic data protection rights (information, access, and objection). It is not possible to break this system down into its components, because one does not function without the others. For instance, one cannot locate in a single legal instrument the principle of security or confidentiality of personal information and, in total lack of any other principle or individual right, establish the existence of a data protection regime. This would be a forced and counter-productive exercise. The absolute international data protection minimum ought to be perceived as a whole: fair information principles and basic individual rights (Europeans would also add an independent monitoring mechanism to this list). If one is missing then no data protection regime exists. **It is from this point of view that we determined that China does not have a data protection regime; instead, it has traces of data protection to be found exclusively in its private sector personal data processing**.

While the above apply to data protection in particular, **the protection of privacy may fare far better under current Chinese law**. As it will be evidenced below, the right to privacy, where however "privacy" is perceived differently in China than in Europe[12], is enshrined in basic Chinese law and indeed at its highest level, ultimately connected to the right to dignity. The presence of privacy protection in China is also facilitated by the fact

[10] See Ess C, *Lost in Translation? Intercultural Dialogues on Privacy and Information Ethics* (Introduction to the special issue on Privacy and Data Privacy Protection in Asia)' (2005) Ethics and Information Technology 7, 1–6.
[11] BBC News, *China surveillance cameras 'a triumph', say police*, 5 October 2015.
[12] See also Ong R, *Recognition of the right to privacy on the Internet in China*, International Data Privacy Law, 2011, Vol. 1, No. 3.

that, unlike the right to data protection, it is not necessary to accompany it with a legal system that effectuates it in practice, but its occurrence is rather established unaided, on an *ad hoc* basis. At any event, while important constraints are evidently applicable in this case as well, because under Chinese law the public sector and national purposes, as dynamically defined by the governing Communist Party, are beyond reach of any law, Chinese individuals have been granted protection by courts on the basis of a violation of their right to privacy. From this point of view, **if data protection was given equal footing as privacy protection, then the "cumulative effect" discussed above would be substantially strengthened**. However this is not the case, at least not in the EU where both the Treaties and extensive case law clearly distinguish between the two. Nevertheless, for the purposes of this analysis and in order to achieve a comprehensive approach, the concept of privacy protection will also be elaborated under the "data protection regime" title.

2.1. The Chinese legal system; democracy and the rule of law in China

A few clarifications on the Chinese legal system are deemed important in order to place the analysis that follows within its appropriate background. China is divided into twenty-two provinces (or, twenty-three if one includes Taiwan), four independent municipalities (Beijing, Shanghai, Tianjin and Chongqing), five autonomous regions (Inner Mongolia, Xinjiang, Guangxi, Ningxia and Tibet), and two special administrative regions (Hong Kong and Macau). Each of these political subdivisions has a central government, regional regulations and a court system. The official structure of the Chinese government was established by its 1982 Constitution. The National People's Congress (NPC) is its highest organ of state power; only it can enact "basic laws" and amend the Constitution. Its permanent body is the Politburo Standing Committee (SC-NPC). It is the second-highest legislative organ in China and has extensive legislative powers, its decisions being legislation.

China's judicial system is described in Articles 123 to 135 of its Constitution: from the top level of the power hierarchy down, the Chinese court system is comprised of the following: the Supreme People's Court, the Higher People's Courts, the Intermediate People's Courts, and the Basic People's Courts. However, it has been found that Chinese courts function more as dispute-resolution mechanisms than like Western-style courts and usually do not issue substantively explanatory decisions but simple rulings which state who wins but not why. When court decisions are lengthy, detailed and more widely released, it is usually because of a specific political agenda; so called "guiding cases" are intended to influence other judges' interpretations of particular laws, but they tend to be few and far between[13]. In particular with regard to the Supreme People's Court its decisions are considered as "authoritative and in practice binding" on lower courts, however it is of limited relevance to the purposes of this report due to the lack of data protection or privacy-relevant cases.

Finally, as far as its political regime is concerned, China is an authoritarian state[14] that is governed by the China's Communist Party. With regard to the rule of law, while noteworthy modernisation attempts have been noted particularly in the past few years[15], it has also been noted that, for the time being, China is a country where "*the concept of rights is so weakly established and the rule of law is hostage to politics*"[16].

[13] All information from Bartow A, *ibid*.
[14] See Greenleaf G, *Asian Data Privacy Laws*, p.20.
[15] See Gao Q/Zhang W/Tian F, *ibid*, pp.103ff.
[16] McCuaig-Johnston M/ Zhang M, *China Embarks on Major Changes in Science and Technology*, China Institute, University of Alberta, 2015, p.29 with further references.

2.2. International data protection obligations and China

In short, China does not carry any international obligations whatsoever with regard to data protection. Although an APEC "member economy", APEC's Privacy Framework is by no means binding to its signatory states. In fact, one should keep in mind that APEC is an organization of states that does not have a constitution or a treaty to establish it but operates by consensus and undertakes commitments on a voluntary basis, claiming to be "the only inter-governmental grouping in the world operating on the basis of non-binding commitments"[17]. APEC "agreements", such as its Privacy Framework, do not have any legal status and are best seen as agreed aspirations, supported by consensus-based commitments to cooperate.

With regard to other international data protection instruments, China is listed among the countries with which the OECD "works closely" within its scope of activities[18], while China is also among the non-member countries where the Council of Europe posts invitations to sign and ratify relevant conventions (its Data Protection Convention being among them)[19], however no formal ratification or even signature within the data protection subject-matter has taken place by China until today. Consequently, in view of the above and in the absence of any other international data protection scheme, China appears until today free of any international data protection obligations.

2.3. Data protection provisions in Chinese legal instruments

As noted above, China does not have a comprehensive data protection law. Instead, a series of sectorial laws has been introduced over the past years, each one of varying legal status, none of which exclusively within data protection subject-matter but rather including some data protection-specific provisions in their texts. Altogether this body of laws could be piled up to formulate a "cumulative" data protection effect. In addition, privacy is protected indirectly, as part of human dignity, in the Chinese constitution and in its basic civil law. For the reasons explained above, none of these data protection traces and look-alikes may be perceived as forming a data protection regime. However, each one of them will be elaborated in the analysis that follows, in order to acquire picture-completeness and to be able to assess the exact dimensions of the cumulative effect discussed with regard to data protection in China. It should be noted that all the analysis below is based on secondary sources.

2.3.1. China's 1982 Constitution. What is the meaning of privacy in China?

China's current Constitution was adopted by the 5th National People's Congress on 4 December 1982 and was subsequently amended in 1988, 1993, 1999, and 2004. It has altogether 138 Articles and is divided into five sections: the preamble, general principles, fundamental rights and duties of citizens, structure of the state, the national flag and the emblems of the state. China's constitution ought not be perceived in the same way as western constitutions. For instance, in its Article 35 it is stated that "*citizens of the People's Republic of China enjoy freedom of speech, of the press, of assembly, of association, of procession, and of demonstration*". In addition, Chinese courts are not allowed to invalidate a statute on the grounds that it violates the constitution nor to enforce its provisions to the benefit of individuals; in fact, its Constitution has been identified as "non-justiciable"[20]. On the other

[17] Greenleaf G, *The APEC privacy initiative: 'OECD Lite' for the Asia-Pacific?* Privacy Laws & Business, Vol. 71, 2004, 16-18.
[18] Information from the OECD website, Directorate for Science, Technology and Innovation.
[19] Information from the Council of Europe data protection website.
[20] Greenleaf G, Asian Data Privacy Laws, p.198.

hand, it should be noted that its amendment in 2004 referred expressly to human rights and to the State's obligation to "*respect and preserve*" human rights (Art.33.3).

There is no data protection-related provision in the Chinese Constitution. Privacy is only referred to once, in particular with regard to "*the freedom and privacy of correspondence*" (Article 40). While it is being argued that "*the Constitution establishes an individual's right to dignity, which under relevant rules is further interpreted to include a right of privacy*"[21], this is not made evident in the Constitution's actual text (the relevant wording in its Article 38 being "*the personal dignity of citizens of the People's Republic of China is inviolable. Insult, libel, false charge or frame-up directed against citizens by any means is prohibited*"). Finally, with regard to case law, it appears that the only case until 2014 what was concerned with the protection of constitutional rights, and was perhaps of some relevance to this report because it concerned identity theft, was later repealed by the Supreme People's Court[22]. Consequently, very little may be derived on any data protection, or indeed privacy protection, regime in China from its Constitution.

While elaborating upon the China's constitutional approach, it is perhaps useful to consider that privacy is not perceived by the average Chinese individual in the same way as in the west. In fact it has been noted that "*privacy remains a strange concept for many in China, and the right to privacy is not an integral part of rights of the person. People have had no clear idea how to distinguish the difference between a shameful secret (yinsi) and privacy (yinsi). These two words were very often used alternately for their pronunciation is almost the same except for a slight difference of the tones*"[23]. This probably explains why, while "*in examining the right to privacy, academics seek to clarify its elements and scope. In this there is evidence of the influence of Western legal scholarship*"[24], Chinese individuals, law and courts continue to mostly associate the right to privacy (no word whatsoever on data protection) with the right to reputation and dignity[25].

2.3.2. Article 253(a) of the Criminal law

According to Article 253(a) of it Criminal law "*Where any staff member of a state organ or an entity in such a field as finance, telecommunications, transportation, education or medical treatment, in violation of the state provisions, sells or illegally provides personal information on citizens, which is obtained during the organ's or entity's performance of duties or provision of services, to others shall, if the circumstances are serious, be sentenced to fixed-term imprisonment not more than three years or criminal detention, and/or be fined. Whoever illegally obtains the aforesaid information by stealing or any other means shall, if the circumstances are serious, be punished under the preceding paragraph. Where any entity commits either of the crimes as described in the preceding two paragraphs, it shall be fined, and the direct liable person in charge and other directly liable persons shall be punished under the applicable paragraph*"[26].

This amendment to Chinese criminal law was enacted in 2009 (amendment VII, 28 February 2009) and has in the meantime become the most widely used provision to enforce privacy protection in China, as it has been used in an estimated minimum of 260 prosecutions

[21] Maisog M/Zhang W, *China* (Chapter 7), in ICLG: Data Protection 2015, Hunton & Williams LLP.
[22] Greenleaf G, *ibid*.
[23] Zhu G, *The Right to Privacy: An Emerging Right in Chinese Law*, Statute Law Review, Volume 18, Number 3, 1997, 208-214.
[24] Ibid.
[25] Ibid.
[26] Unofficial translation from the UN Office on Drugs and Crime, available at https://www.unodc.org/tldb/pdf/ChineseLegislation/China_Criminial_Law_Amendment_VII_EN.pdf

until 2014[27]. Essentially, it refers only to the illegal sale or purchase of personal data. In the first case, that of the sale or illegal provision of personal data, its addressees are employees in state or private sector agencies. With regard to the illegal obtaining of the same data its addressees do not necessarily include employees of the above agencies, but instead any person – this after all is the legal reasoning behind China's most noted case in privacy protection, the *Roadway case* discussed below under 2.4. In this context, it appears that, to-date, Chinese courts have interpreted narrowly Article 253(a)1's prohibition on illegal sale or provision, restricting its application solely to state entities and other public facing industries. However, they have given Article 253(a)2 a broad interpretation, applying it to illegal obtainment of personal information by any individual or entity, regardless of their particular industry, and apparently without the need for a preceding prosecution under Article 253(a)1 or for the information to have originated from an Article 253(a)1 listed-entity[28].

In addition to the above, other provisions in the Chinese criminal law that were enacted under the same Amendment (VII) in its Article 285 refer to "*computer information systems*" crimes, such as "*intrusions*" or "*illegal control*" over them. These provisions, to the extent that personal data are stored in such information systems could also be used within a data protection context.

2.3.3. Civil law: Article 101 of the General Principles of Civil Law and Article 2 of the Tort Liability Law

The civil law framework in China includes separate legislative acts: the General Principles of Civil Law (1986), Contract Law (1999), Property Law (2007) and the Tort Liability Law (2009). However, of relevance to the purposes of this report are only the General Principles of Civil Law and the Tort Liability Law.

With regard to the former, the General Principles of Civil Law do not include any explicit mention to a data protection or privacy right but rather a general right to reputation: "*Citizens and legal persons shall enjoy the right of reputation. The personality of citizens shall be protected by law, and the use of insults, libel or other means to damage the reputation of citizens or legal persons shall be prohibited*" (Article 101)[29]. Other Articles protect specifically an individual's right of personal name, portrait, and honor (Articles 99, 100 and 102, respectively). Despite of the lack of specific provisions, "decided cases suggest that it does provide some privacy protection"[30]. In particular, it appears that the Supreme People's Court has traditionally (since 1988) treated various forms of disclosure of personal information as a potential infringement of the above right to reputation (if indeed the same individual's reputation has been harmed in the process)[31].

On the other hand, the Tort Liability Law, that was the latest addition to the Chinese civil law as it came into effect only in 2010, holds an important part in the Chinese data protection (or, better, privacy protection) regime, because it expressly refers to a right to privacy in its list of protected "civil rights and interests". According to its Article 2, "*those who infringe upon civil rights and interests shall be subject to the tort liability according to this Law. "Civil rights and interests" used in this Law shall include the right to life, the right to health, the right to name, the right to reputation, the right to honor, right to self-image, right of privacy, marital autonomy, guardianship, ownership, usufruct, security interest,*

[27] Livingston S/Greenleaf G, *China Whys and wherefores – Illegal provision and obtaining of personal information under Chinese law*, 131 Privacy Laws & Business International Report, 2014.
[28] Ibid.
[29] See Bu Y, *Defamation*, in Bu Y (ed.), Chinese Civil Law, C H Beck – Hart – Nomos, 2013.
[30] Greenleaf G, Asian Data Privacy Laws, p.200.
[31] Ibid, with further references.

copyright, patent right, exclusive right to use a trademark, right to discovery, equities, right of succession, and other personal and property rights and interests"[32]. Separate mention is reserved in the same law's text to medical institutions and their patients' "privacy" (in Article 62A). However, nowhere in Tort Liability Law is a definition of such "right to privacy" to be found. While the short period since its release means that no time for significant case law has been available, it has been found that "examples of the very few known actions under article 2 of the TLL indicate that it is primarily being used to resolve disputes between individuals, rather than against corporations"[33].

Finally, special mention needs to be made to Article 36 of the same Tort Liability Law, where it is mentioned that "*a network user or network service provider who infringes upon the civil right or interest of another person through network shall assume the tort liability. Where a network user commits a tort through the network services, the victim of the tort shall be entitled to notify the network service provider to take such necessary measures as deletion, block or disconnection. If, after being notified, the network service provider fails to take necessary measures in a timely manner, it shall be jointly and severally liable for any additional harm with the network user. Where a network service provider knows that a network user is infringing upon a civil right or interest of another person through its network services, and fails to take necessary measures, it shall be jointly and severally liable for any additional harm with the network user*". Therefore, by means of direct mention to the "*civil rights and interests*" list of Article 2, where the right to privacy is expressly included, Chinese "network users" or "network service providers", who could be interpreted as including internet users and ISPs, are threatened with tort liability in the event of a privacy infringement. The responses of deletion, blocking or disconnection are expressly mentioned in the law. This provision, that ultimately resembles the providers' liability provisions of the e-Commerce Directive[34], could also be placed within the broader personal data protection framework. However, until 2014 apparently little use had been made of this Article, hence China's Supreme People's Court Regulation, released in October 2014 entitled "*The Supreme People's Court Regulations Concerning Some Questions of Applicable Law in Handling Civil Dispute Cases Involving the Use of Information Networks to Harm Personal Rights and Interests*"[35], whose use in practice however remains to be established.

2.3.4. The *de facto* data protection standard on the internet: the 2012 SC-NPC Decision

The Standing Committee of its National People's Congress (SC-NPC), as already seen, is China's second-highest legislative organ, its decisions effectively constituting legislation. In 2012 the Committee released its "Decision on Internet Information Protection" (the "2012 SC-NPC Decision"). This decision is until today the highest level law in China to deal specifically with data protection issues. Because all other relevant legislation, such as the Ministry of Industry and Information Technology initiatives that are discussed immediately below, has to conform to it, and because the Decision is the only Chinese data protection legal instrument to also apply to the public sector as well, it is considered the *de facto* data protection standard in China.

The SC-NPC Decision is composed of altogether 12 articles and is aimed at protecting "electronic information", as per its Article 1, which effectively means that, in certain provisions, its protection may be broader than the internet only as suggested by its title. The protec-

[32] See also Bu Y, *General Provision on Tort Liability*, in Bu Y, *ibid*, pp.143ff.
[33] Ibid, p.202.
[34] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce'), OJ L 178, 17.7.2000, 1–16.
[35] See also Livingston S/Greenleaf G, *The emergence of tort liability for online privacy violations in China*, 135 Privacy Laws & Business International Report, 2015, 22-24.

tion of individual privacy is explicitly referred to, also in its Article 1. The Decision's addressees are "*internet service providers and other enterprises and institutions that collect or use citizens' personal electronic information in the course of their business*". These "*shall abide by the principles of legality, legitimacy and necessity, clearly indicate the objective, methods and scope for collection and use of information, and obtain agreement from the person whose data is collected, they may not violate the provisions of laws and regulations, and the agreement between both sides, in collecting or using information*" (Article 2). The confidentiality and security of processing are equally protected (in Articles 3 and 4 respectively). "Real identity information" is to be requested by all network service providers when providing online or telecommunications services (Article 6). Data subjects are afforded the right, when they discover infringement of their rights, to ask data controllers to "delete the information" or "cease the infringement" or "report to the controlling departments" (Articles 8 and 9).

If the 2012 SC-NPC Decision was to be judged against the EU data protection model, its shortcomings would become easily evident in the sense that it is lacking in scope (internet only), in enforcement mechanism (none whatsoever), in basic data subject rights (none whatsoever), as well as, in its principle-setting (their list does not include all of the principles in the EU data protection approach). However, if it is viewed as a first attempt towards a comprehensive data protection regime, then the Decision does present certain merits, mostly in the form of basic data protection elements that may be found in its text. In addition, its high-level origin means that it sets the *de facto* standard in the internet-related personal data processing field. Other Chinese agencies were quick to pick up on this new development: in fact, the Decision's key terminology (meaning the general principles set out in Article 2) have been adopted in other legislation that followed it, such as the 2013 MIIT Regulations and the 2013 amendments to China's Consumer Law, that will be discussed in the analysis that follows.

2.3.5. The data protection framework for internet and telecommunications providers: the 2011 MIIT Regulations, the 2013 MIIT Guidelines and the 2013 MIIT Regulations

The basis of China's sectoral approach to data protection is apparently to be found on the regulatory work that has been undertaken in this field by the Chinese Ministry of Industry and Information Technology (MIIT) over the past few years. In practice, within the past five years it has issued two sets of Regulations (the latter not repealing the former) as well as a set of Guidelines that are all aimed at regulating the internet and the telecommunications field. While their scope is limited only to that sector of personal data processing, and in any event the general exemption of the public sector ought to be kept in mind, the fact remains that all these instruments present strong data protection characteristics that resemble, but not equal, in many respects the level of protection afforded to individuals by the OECD Guidelines.

As far as the 2011 MIIT Regulations ("Several Regulations on Standardizing Market Order for Internet Information Services") are concerned, they were adopted as a Decree of the MIIT on 7 December 2011 and came into effect on 15 March 2012. Because no official or unofficial English translation may be found on the internet, the analysis focuses on secondary sources only. The Regulations are addressed to "Internet Information Services Providers" (IISPs), meaning "*all those that are engaged in internet information services and/or activities relating to internet information services*" in China[36]. This had been apparently been interpreted to include any and all parties providing information to internet users over the internet[37]. The 2011 MIIT Regulations include data protection-relevant provisions, such as the personal data processing principles (in Articles 11-14), collection limitations and notification, data breach notifications (to the authorities), as well as data exports limitations[38].

[36] Greenleaf G, *Asian Data Privacy Laws*, p.205.
[37] Ibid.
[38] See Greenleaf G, *China's Internet data privacy Regulations 2012: 80% of a Great Leap Forward?* Privacy Laws & Business International Report, Issue 116, 2012, 1-5.

Overall, it has been found that the 2011 MIIT Regulations, while they "*fall short of all international standards because of their lack of access and correction rights, and their limited scope to Internet information providers, it meets the basic standards of the principles in the OECD Guidelines in many other respects. The other significant place at which it falls short is that the limitations on disclosure only apply to user-provided personal data, and not that which has been collected from third parties or generated from transaction. In a few respects (minimal collection; data breach notification), the Regulation includes more recent privacy principles. It is a very significant step for China, even if it would be a very limited one in other countries*"[39].

The 2013 MIIT Guidelines, while voluntary in nature, are considered important because of their scope that extends to any "*processing of personal information through information systems*" (meaning therefore all networks and not necessarily the internet), as well as because of the fact that they cover in detail such key issues as data exports, sensitive data, data subject access and the right to rectification[40]. The 2013 Guidelines were in fact released by the MIIT Standardisation Administration in a format that is generally "intended for situations where formal standards are premature"[41]. Overall, their significance remains "mysterious" with authors since their release speculating whether they will continue having a "shadowy existence" or whether they will be elevated into being "a model for a future Chinese data protection law, once an enforcement mechanism is added"[42]. Until today there appears to exist no evidence towards any one of the above directions.

Finally, the 2013 MIIT Regulations are broader in scope than their 2011 equivalent, because they are addressed to IISPs and "telecommunications business operators" (Article 2). In fact, the 2013 MIIT Regulations constitute implemented measures for the 2012 SC-NPC Decision. However, their relationship to the 2011 Regulations of the same Ministry is ambivalent, given that, while they do not expressly replace them, it is stated in their text that their provisions on notice and consent supersede any other law or regulation on this topic (in Article 9). At any event, the 2013 MIIT Regulations include definite data protection-relevant provisions: among others, they include a definition of "personal data" (in Article 4), they refer to the principles of "legality, propriety and necessity" (in Article 5), to user consent (in Article 9), to data breach notifications (to the authorities only, in Article 14), or to supervision (by state authorities, in Article 17) and provider liability (fines, to be imposed by state authorities, in Article 22). Consequently, if they are placed within their proper framework, together with the 2011 Regulations, the 2013 Guidelines and, of course, the 2012 SC-NPC Decision, the 2013 Regulations formulate a more or less complete data protection legal regime for the internet and telecommunications sector in China, given of course the general-applying limitations in all relevant legislation in China (state exemption, no independent enforcement mechanism, no individual rights)[43]. Regardless of these shortcomings, the fact remains that the telecommunications and internet fields are, for the past few years, more or less accustomed to abiding by data protection rules – a useful practice that could find broader application in the future.

2.3.6. Data subjects as consumers but with data protection rights: The 2013 SC-NPC amendments to the Law on the Protection of Consumer Rights and Interests. The Chinese data protection "cumulative" effect

[39] Ibid, p.7.
[40] Greenleaf G, *Asian Data Privacy Laws*, p.207.
[41] Ibid.
[42] See Greenleaf G, *ibid*, Greenleaf G/Tian G, *China Expands Data Protection Through 2013 Guidelines: A 'third line' for personal information protection*, Privacy Laws & Business International Report, Issue 122, 2013, 4-6, Livingston S, *China Releases National Standard for Personal Information Collected Over Information Systems; Industry Self-Regulatory Organization Established*, Inside Privacy, 2013.
[43] See Greenleaf G, *China's incremental data privacy law: MIIT 'User Data Protection' Regulations, 2013*, 125 Privacy Laws & Business International Report, 2013, 18-19.

China's "Law on the Protection of Consumer Rights and Interests" was entered in 1993. Its first major amendment took place in 2013 and came through a decision of China's Standing Committee of its National People's Congress (SC-NPC), effectively the same body that released the 2012 SC-NPC Decision discussed above on "Internet Information Protection".

The Committee was consistent with its 2012 approach on data protection and in 2013 it included in the amendment of China's basic consumer law data protection provisions that were almost identical to the ones included in its 2012 Decision. Effectively, the amendment repeated Article 2 of the 2012 SC-NPC Decision in its (codified) Article 29. In addition, in its Article 50 it is stated that "*proprietors who harm consumers' human dignity, infringe upon consumers' personal freedom or upon consumers' lawful right to protect personal information, shall cease infringement, restore consumers' reputation, eliminate the impact, make formal apologies, and compensate consumers for losses*". A monetary fine, among others when "*the human dignity or personal freedom of consumers is infringed or consumers' lawful right to protection of their personal information is infringed*", is subsequently set in Article 56.

As was the case above with regard to the 2012 SC-NPC Decision, if judged from a data protection point of view the amended Chinese consumer law could not possibly amount to a data protection regime, because it is missing both in scope (purpose of the legislation) as well as in principles, rights and enforcement mechanism. However, the above development is important in at least two ways. First, because of its broad scope (consumer law covers both the online and the off-line world) data subjects, viewed as consumers, are practically provided with some level of data protection in all their relationships with the private sector. And, second, by repeating its previous wording and expanding it into the offline world as well, China's second highest legislative body, the SC-NPC, confirmed its law-making approach on the matter as laid down in its 2012 Decision.

It is in this regard that one could talk of a "cumulative effect"[44] of Chinese data protection law, meaning that, if one adds up the 2012 and the 2013 SC-NPC Decisions, then the whole of China's private sector personal data processing is in one way or another regulated (with the internet and telecommunications sectors profiting from the more detailed work undertaken by the MIIT). Individuals may also recur to civil law or even criminal law protection, if qualifying circumstances are met. While this is a worthy attempt, the rationale that led to such cumulative effect (the protection of commerce, rather than human rights) together with the shortcomings discussed above (state exemption for most of the above provisions, no independent enforcement mechanism, no individual rights) leave in effect little space for an actual legal assessment of this statement. In other words, while data protection-like provisions may be applicable in several processing circumstances in China today, these do not amount to or replace a comprehensive data protection regime. In addition, their effectiveness in practice, when applied by courts or other authorities, for the benefit of these individuals that they are supposedly released to protect remains if not doubtful then to be established in the future.

2.3.7. Other regional and provincial laws

China's complex legal system allows to its provinces, regions and even cities to introduce special legislation applicable only within their jurisdictions. In this context many among them have chosen to enact either dedicated data protection-relevant legislation (see, for instance, the Jiangsu Province's Regulation of Information Technology or Xuzhou City's Municipal Provisions for Protection of Computer Information System Security) or to introduce data protection provisions in otherwise unrelated legal acts (see, for instance, Shanghai's Consumer Protection Rules or Henan Province's Information Ordinance)[45]. Given that each

[44] See Greenleaf G/Tian G, *Data Protection Widened by China's Consumer Law Changes*, 126 Privacy Laws & Business International Report, 2013, 127-28.
[45] All information from Greenleaf G, *Asian Data Privacy Laws*, p.223-224.

one of China's political subdivisions has a local court system, it is not unlikely that relevant local case law has also developed. To this end, foreign enterprises wishing to become active in China are customarily advised to conduct a local legal inquiry, as to what exactly legislation is applicable on their activities. However, with regard to the purposes of this report reference here to these local legal acts is only made in order to demonstrate the complexity of the system and the lack of information at local level. At any event, it is not to be expected that any local legislation will have surpassed the boundaries set by central government in the basic decisions in the field, namely the 2012 SC-NPC Decision and the 2013 SC-NPC amendment to China's basic Consumer Law, as discussed above.

2.3.8. The (abandoned) 2007 draft general Data Protection Bill

In 2007 a comprehensive draft Personal Information Protection Act was apparently under consideration in China, but never made it through the law-making process. Had it been adopted, it would have provided China with an actual data protection instrument that would have covered both the public and private sectors and would have included a "reasonably comprehensive set of data privacy principles", although not an independent data protection authority as well[46]. Anyway, the draft Bill never managed to become an Act in China and its relevance today may be found only through comparison between its ambitious approach and what has actually been implemented in China ever since.

2.4. Relevant case law

There is yet limited case law with regard to data or privacy protection afforded to individuals in China. Court actions on the basis of legislative acts enacted since 2012 need more time to conclude and to become public. Until today a limited number of cases referring directly or indirectly to privacy protection have been known, perhaps the most notable of which referring to the *Qi Yuling v Chen Xiaoqi* (identity theft), the *Wang Fei* (internet shaming), as well as to the *Shanghai Roadway* (criminal prosecution) cases[47].

In the first case, the defendant apparently stole the plaintiffs identity in order to obtain admission and pursue her studies in higher education. The matter was ultimately referred to the SPC, that ruled in favor of the plaintiff on the basis of infringement of her constitutional rights – a first, because until then constitutional rights were not justifiable on the basis of civil liability. However, the SPC withdrew its opinion, stating that it was no longer applicable, a few years later. In the second case, Wang Fei was tracked down and harassed because of an internet shaming campaign launched by a friend of his late wife, who committed suicide because of his extramarital affair. The court vindicated his claim on the basis of civil law (the General Principles, because Tort Liability was not enacted yet) and imposed fines on the defendant as well as on these internet providers that failed to remove the information after his petition.

Finally, in the third case, a local subsidiary of an international firm was heavily fined and four of its executives were imprisoned for illegally buying information on (150 million) Chinese consumers. This was a criminal prosecution case, on the basis of Article 253(a) of the Chinese Criminal Law. Apparently, until today this is the preferred way forward in order for Chinese individuals to protect their right to their personal information. Some civil actions under the Tort Liability Law are also occurring[48]. Given however the fact that no central registry, or case law analysis exist until today, all evidence on case law within the data protection or privacy field remain circumstantial and could not lead to credible results[49].

[46] See Greenleaf G, *Asian Data Privacy Laws*, p.208, Greenleaf G, *China's Proposed Personal Information Protection Act*, Privacy Laws & Business International Newsletter Issues 91 and 92, 2008, Zhu G, *ibid*.
[47] See also Xue H, *Privacy and personal data protection in China: An update for the year end 2009*, Computer Law & Security Review, 26 (2010) 284–289.
[48] See Greenleaf G, *Asian Data Privacy Laws*, p.226.
[49] Ibid.

3. GENERAL ASSESSMENT OF THE DATA PROTECTION REGIME IN CHINA

KEY FINDINGS

- An assessment of the data protection regime in China would be an impossible task because the fundamentals of international data protection (a set of basic data processing principles, the fair information principles, and a set of basic data protection rights – information, access, rectification) are not unequivocally warranted in China. To that list Europeans would also add adequate means of enforcement that are however also not provided for under Chinese law.
- Since there is no data protection authority or any other state agency to monitor the protection of personal data, courts are apparently the only viable remedy for the protection of individuals in this regard. However, until sufficient time has passed in order for legal acts of the past five years, particularly in China's Civil Law, to demonstrate their full potential for the data protection purposes, the role of courts as an enforcement mechanism remains questionable.
- While assessing the Chinese approach to data protection, the basic terms of reference of any relevant instrument ought to be kept in mind: (a) Human rights, at least as known in western countries, are not protected in China, (b) The public sector, and all state aims and purposes as dynamically defined by China's ruling Communist Part from time to time, should generally be perceived as exempted from all legislation, and (c) Court decisions do not lead to legal certainty.
- The actual wording that supports any Chinese claim on the protection of personal data processing, constituting in essence the premises for China's much-discussed data protection "*cumulative*" effect, is limited to the following obligations of data controllers: "*[to adhere to] the principles of legality, legitimacy and necessity, clearly indicate the objective, methods and scope for collection and use of information, and obtain agreement from the person whose data is collected, […] not violate the provisions of laws and regulations, and the agreement between both sides, in collecting or using information*".
- Among the biggest shortcomings of the Chinese data protection system may be listed the lack of common definitions, the lack of the notion of individual consent, the lack of any mention to the rights of information, access and rectification, as well as the lack of a supervising state authority (not necessarily an EU-style data protection authority but even a USA-like federal trade commission).

An assessment of the data protection regime in China would be an impossible task because, as evidenced above, there is none to be found. This finding is based not only after comparison to the, perhaps strict and formal, EU data protection model but also when analyzing what Chinese legislation exists on this matter against the more flexible models of the Council of Europe or the OECD or even against the absolutely minimum data protection international common standards. These minimum international common standards pertain to the fair information principles and to the special data subject rights. Europeans and most countries (and legal scholars) around the world would also add adequate means of enforcement to this list as well.

The fair information principles include the fair and lawful collection and processing of personal information, the proportionality of the processing, data minimization, the purpose specification principle, data security and data confidentiality. Admittedly this is the criterion where China fares best with regard to its data protection regime: after the 2012 SC-NPC

Decision, that regulated all of the internet, and in particular its Article 2 that was subsequently included as such in the 2013 amendment of China's basic Consumer Law, undertaken by the same committee, by now China's whole private sector has to abide by the principles of "*legality, legitimacy and necessity, clearly indicate the objective, methods and scope for collection and use of information, and obtain agreement from the person whose data is collected, they may not violate the provisions of laws and regulations, and the agreement between both sides, in collecting or using information*". This list is even more detailed in regulations applicable on the internet and telecommunications sectors only (a combined reading of the MIIT 2011 Regulations, 2013 Guidelines and 2013 Regulations is required to this end). Although this is an important development, even a simple comparison between this wording and the list of principles mentioned above demonstrates the Chinese implementation's shortcomings in this regard.

The data subject rights of information, access and rectification are crucial to any data protection regime. They afford individuals with the means to be informed that data on themselves are being processed, to have access to such data and, after filing a lawful request, to make corrections and amendments if justified. None of these rights exist in any Chinese data protection-related legal text.

Finally, an effective enforcement mechanism (ideally in the form of an independent agency such as a data protection authority, but even any state agency, such as USA's Federal Trade Commission or even any systematic case law would probably be assessable to this end) is also a basic data protection component. While there is nothing similar or even remotely close to a data protection authority in China even within the internet and telecommunications sector that is otherwise at the forefront of data protection regulation, Chinese courts also do not appear until today to suggest a viable solution, at least from the legal certainty point of view. The limited case law that is available borders with the right to reputation or identity theft; already the SC-NPC has repealed its approach on an important case, bringing constitutional rights back to non-justiciability in civil cases; the harshest and most pertinent to data protection conviction came from the field of criminal law and was imposed on a foreign subsidiary. Consequently, until sufficient time has passed in order for legal acts of the past five years, particularly its civil law, to demonstrate their full potential for the data protection purposes, the role of courts as an enforcement mechanism in this regard remains questionable.

After all, China does not qualify as a country with a data protection regime even under Greenleaf's more flexible approach ("*a national law which provides, in relation to most aspects of the operation of the private sector, or its national public sector, or both, a set of basic data privacy principles, to a standard at least including most of the OECD Guidelines or Council of Europe Convention, plus some methods of statutorily mandated enforcement (i.e. not only self-regulation*), that has helped him raise the number of qualifying countries around the globe to 109. However, even under this relatively relaxed approach still China does not make it into the list.

What therefore remains is a data protection approach rather than a data protection regime. China has implemented data protection-related provisions in several personal data processing sectors over the past decade. While these provisions do not amount to a comprehensive data protection regime, they may still be evaluated within their own terms of reference. In particular, these terms of reference include the following facts:

(a) Human rights, at least as known in western countries, are not protected in China;
(b) The public sector, and all state aims and purposes as dynamically defined by China's ruling Communist Part from time to time, should generally be perceived as exempted from all legislation;
(c) Court decisions do not lead to legal certainty.

Given the above and in view of the analysis under Chapter 2 above, the basic characteristics of what data protection provisions are in place in China until today may be summarized as follows:

(i) There is no formal distinction between the right to privacy and the right to data protection. The right to privacy may be derived from the Chinese Constitution or civil law but it should be noted that in China it is interpreted differently than in the EU, being intrinsically connected to reputation and human dignity;
(ii) A right to the protection of personal information (data protection) apparently applies over all private sector processing in China, at least under combined reading of China's basic consumer and internet law texts;
(iii) However, the purpose and content of such right to the protection of personal information is security or public trust in commerce and not the protection of a human right;
(iv) The wording that supports such right to the protection of personal information in China, and in essence constitutes the premises for China's much-discussed data protection "cumulative" effect, is practically limited to the following obligations of data controllers: "[to adhere to] *the principles of legality, legitimacy and necessity, clearly indicate the objective, methods and scope for collection and use of information, and obtain agreement from the person whose data is collected, […] not violate the provisions of laws and regulations, and the agreement between both sides, in collecting or using information"*;
(v) Combined reading and legal reasoning are key in order to approach China's data protection regime: its Constitution needs to be read in such a way as to include a right to privacy that does not exist in its wording; its SC-NPC Decisions need to be read in conjunction in order to formulate the greater picture that all of China's private sector has to abide by some data protection provisions. Nevertheless, both these intellectual exercises (combined reading and legal reasoning) may well prove to be in practice no more than western wishful thinking in an otherwise circumstantial and elusive data protection approach within an authoritarian state[50].

Consequently, while an assessment of China's data protection regime would be impossible, an identification of its most serious shortcomings, even within the above three terms of reference that apparently ought to be taken for granted, would perhaps be useful in order to formulate the policy recommendations that follow (under 4):

(1) Even within what data protection legislation exists in China there are no common definitions. For instance, there is no indication on what is "personal information", what is "processing", or who are the actors in such processing, meaning what are the definitions for "data controllers", "data processors" and "data subjects". This is true even within the internet and telecommunications sectors, that benefit from more extensive regulation;

(2) The notion of consent is central to data protection both in and out of the EU. While reference to consent is made in the standard data protection provisions employed in China until today, no further clarifications are provided as to its exact characteristics (what exactly it includes, how it is given, how it is established, etc.);

(3) The rights of information, access and rectification are equally central in the data protection environment but they do not exist under current Chinese legislation, even in the fields of the internet or telecommunications;

[50] In this context it has been noted that "*At present, Chinese legalism faced another antithesis, The Western Rule of Law ideology. Western theorists might misunderstand Chinese legalism. They might use the concept of Western legalism to cover Chinese legalism incorrectly because of the English translation*" (He P, *Chinese Lawmaking: From Non-communicative to Communicative*, Springer, 2014.

(4) There is no formal and accessible way of judicial redress for individuals. Until today claimants have mostly made use of a dedicated article in China's basic Criminal Law; Tort Liability Law, enacted in 2009, still waits to show its full potential. However, in what formal data protection texts do exist (in the internet and telecommunications sector) no reference is made to judicial redress, but rather to recourse to the competent administrative authorities, a supposedly less appealing solution that also does not appear to provide to the individuals whose rights were infringed with concrete results;

(5) While it is obvious that a data protection authority is missing and no plans exist to establish one in the foreseeable future, what is less obvious is that little guidance is provided to individuals even as to the competent administrative authorities they may turn to in case that their rights have been infringed. In essence, all data protection-relevant texts refer to such authorities not by name but in general terms ("*the relevant administrative authorities*"). Because the field of application may vary significantly (internet, telecommunications, consumer law), regional or provincial legislation may also apply, while important legislation usually comes from a central committee (the SC-NPC), identifying which authority is competent each time for individuals to address themselves in case of infringement of their rights ought not be considered a self-evident task;

(6) Data breach notifications are indeed applicable in certain fields under the Chinese data protection regime but they are rather "introvert", meaning that data controllers are supposed to alert authorities only and not the individuals concerned;

(7) Given the complexity of China's legal system particularly at local (regional and provincial) level, if practical results were aimed at a legal inquiry on any data protection-relevant legislation at local level would be necessary; however, the significance of such fragmentation need not be overestimated, given the strict boundaries set in the basic SC-NPC Decisions in the field.

4. POLICY RECOMMENDATIONS

KEY FINDINGS

- Our suggested policy options are based on a realistic rather than a legalistic approach.
- If a legalistic approach was adopted, then no common grounds could be found between two fundamentally different systems both in their wording and in their *raison d'être*. In addition, data transfers would need to be prohibited towards China, on the basis of Article 25 of the EU 1995 Data Protection Directive. However, this would be an impractical, if not unnecessary position. Over the past few years China has enacted a series of data protection-related legal texts; this initiative need not be discouraged but rather strengthened and tested.
- Personal data flows between the EU and China might become a pressing reality in practice within contemporary cloud computing environments, where vast data centres may be installed (or are already operating) in China.
- We therefore believe that, while commercial and other relationships need not be stifled on data protection grounds, concrete and specific policy recommendations need to be provided to China. Thus, China would have the opportunity to demonstrate that its recent data protection effort is part of a persistent, yet concise, policy and not just a pretext to attract more internal and external information processing business.
- To this end a list of policy recommendations has been drawn up with regard to (a) the basic data protection principles, (b) the basic data protection individual rights, (c) data transfers, and (d) the enforcement mechanism.

In view of the above findings, we have drawn up the following policy recommendations, based on a realistic rather than a legalistic approach. If a legalistic approach was adopted, then no common grounds could be found between two fundamentally different systems both in their wording and in their *raison d'être*. In addition, data transfers would need to be prohibited towards China, on the basis of Article 25 of the EU 1995 Data Protection Directive. However, this would be an impractical, if not unnecessary position. Over the past few years China has enacted a series of data protection-related legal texts; this initiative, although far from the 2007 comprehensive Data Protection Bill approach, need not be discouraged but rather strengthened and tested.

In addition, personal data flows between the EU and China might become a pressing reality in practice within contemporary cloud computing environments, where vast data centers may be installed (or are already operating) in China. Indeed, China has adopted an aggressive commercial policy to this end, constructing an "International Offshore Cloud Computing Zone" in Chongqing and opening up the Shanghai Free Trade Zone to foreign investors. Already companies such as Microsoft, IBM and Amazon are preparing to participate in its cloud infrastructure[51]. On 22 July 2015 Aliyun (Alibaba's cloud computing subsidiary), issued a Data Protection Pact while releasing its cloud products to the Chinese market[52].

We therefore believe that, while commercial and other relationships need not be stifled on data protection grounds, concrete and specific policy recommendations need to be provided to China. Thus, China would have the opportunity to demonstrate that its recent data pro-

[51] China Briefing, *Foreign IT Giants Rush to Tap China's Cloud Computing Market*, 3 February 2015.
[52] BusinessWire.com, *Alibaba's Aliyun Initiates Data Protection Pact for Worldwide Cloud Consumers at Its Inaugural Data Technology Day*, 22 July 2015.

tection effort is part of a persistent, yet concise, policy and not just a pretext to attract more internal and external information processing business.

Given the above, the following list of policy recommendations has been drawn up:

A. With regard to the basic data protection principles:

(1) A set of common definitions (what is "personal information", "processing", the actors of processing and their roles etc.) could be introduced in the SC-NPC Decisions (of 2012 on internet processing and 2013 on consumer law);

(2) The list of processing principles as set Article 2 in the SC-NPC Decision (and repeated in the consumer law amendment of the same committee) could be expanded to reflect, if not these of the EU Data Protection Directive, then at least these of the Council of Europe Data Protection Convention or even these of the OECD Guidelines;

(3) The notion of consent could be introduced, at least in private sector personal data processing (again, by means of insertion into the above two SC-NPC Decisions);

(4) An effort could be undertaken to extend the scope of data protection instruments also to the public sector or at least to these state agencies that are not crucial to the central state government purposes.

B. With regard to the basic data protection rights afforded to data subjects:

(1) The rights of information, access and rectification are central in the data protection environment in all international data protection regulatory models (EU, CoE, OECD, APEC) and there is no apparent reason why they are not expressly granted to Chinese individuals as well, given that the SC-NPC Decisions already in place grant them the right to request data controllers "*to cease infringing their rights*";

(2) A discussion on the "right to be forgotten" could be of relevance in China particularly with regard to the 2012 SC-NPC Decision on Internet Information Protection, given also the Chinese tendency to connect the right to data protection to the right to privacy and, ultimately, to the rights of reputation and human dignity.

C. With regard to data transfers:

(1) Given Chinese plans to host a substantial part of the global cloud computing capacity within China, it is important to open discussions on exactly what such a development means for EU personal information. While international cloud transfers to China could evidently not be regulated under an EU "*adequacy*" finding, the remaining EU alternatives ought to be examined: model contracts or binding corporate rules. Given China's size and importance, an option similar to the *Safe Harbor* policy adopted with the USA would not appear extreme. Such a development would ultimately benefit both Europeans and Chinese individuals;

(2) China's "International Offshore Cloud Computing Zone" in Chongqing and even the Shanghai Free Trade Zone, whose ambition is to become a global player in cloud computing could benefit from case-specific increased data protection regulations, in the form of a local law, that match the stricter international data protection regulatory models of the EU or the CoE;

(3) Adherence by Chinese corporations involved in cloud computing to the recent cloud computing standard ISO/IEC 27018 could provide additional safeguards.

D. With regard to the enforcement mechanism

(1) While an independent state data protection authority may not be well-suited under contemporary circumstances in the Chinese administrative edifice, a registration or prior notification system could be set up even within a specific sector within a specific ministry (the MIIT, with its active role in regulation until today easily comes to mind);

(2) Chinese legal instruments could identify the "competent authorities" to which individuals may address their complaints, rather than refer to them in abstract, in order to enhance individual redress;

(3) Given local fragmentation and difficulty of tracing resources, an effort could be undertaken by the Chinese government: (a) to create a central internet repository of all data protection and privacy instruments in effect both at central government level and per region; and (b) to provide an official English translation of all these legal instruments as well as any basic case law, if applicable.

REFERENCES

- Bartow Ann, *Privacy Laws and Privacy Levers: Online Surveillance versus Economic Development in the People's Republic of China*, 74 OHIO ST. L.J. 853, 2013.
- Bu Y (ed.), *Chinese Civil Law*, C H Beck – Hart – Nomos, 2013.
- Ess C, *Lost in Translation? Intercultural Dialogues on Privacy and Information Ethics* (Introduction to the special issue on Privacy and Data Privacy Protection in Asia) Ethics and Information Technology 7, 2005, 1–6.
- Gao Q/Zhang W/Tian F, *The Road to the Rule of Law in Modern China*, Springer, 2015.
- Greenleaf G, *Global data privacy laws 2015: 109 countries, with European laws now a minority*, 133 Privacy Laws & Business International Report, February 2015.
- Greenleaf G, *Asian Data Privacy Laws: Trade & Human Rights Perspectives*, Oxford University Press, 2014.
- Greenleaf G/Tian G, *China Expands Data Protection Through 2013 Guidelines: A 'third line' for personal information protection*, Privacy Laws & Business International Report, Issue 122, 2013, 4-6.
- Greenleaf G/Tian G, *Data Protection Widened by China's Consumer Law Changes*, 126 Privacy Laws & Business International Report, 2013, 127-28.
- Greenleaf G, China's incremental data privacy law: MIIT 'User Data Protection' Regulations, 2013, 125 Privacy Laws & Business International Report, 2013, 18-19.
- Greenleaf G, *China's Internet data privacy Regulations 2012: 80% of a Great Leap Forward?* Privacy Laws & Business International Report, Issue 116, 2012, 1-5.
- Greenleaf G, China's Proposed Personal Information Protection Act, Privacy Laws & Business International Newsletter Issues 91 and 92, 2008.
- Greenleaf G, *The APEC privacy initiative: 'OECD Lite' for the Asia-Pacific?* Privacy Laws & Business, Vol. 71, 2004, 16-18.
- He P, *Chinese Lawmaking: From Non-communicative to Communicative*, Springer, 2014.
- Lee J-A, *Regulating Blogging and Microblogging in China*, Oregon Law Review, Vol. 91, No. 2, 2012.
- Livingston S/Greenleaf G, *The emergence of tort liability for online privacy violations in China*, 135 Privacy Laws & Business International Report, 2015.
- Livingston S/Greenleaf G, *China Whys and wherefores – Illegal provision and obtaining of personal information under Chinese law*, 131 Privacy Laws & Business International Report, 2014.

- Livingston S, *China Releases National Standard for Personal Information Collected Over* Information Systems; Industry Self-Regulatory Organization Established, Inside Privacy, 2013.
- Maisog M/Zhang W, *China* (Chapter 7), in ICLG: Data Protection 2015, Hunton & Williams LLP.
- McCuaig-Johnston M/ Zhang M, *China Embarks on Major Changes in Science and Technology*, China Institute, University of Alberta, 2015, p.29 with further references.
- Ong R, *Recognition of the right to privacy on the Internet in China*, International Data Privacy Law, 2011, Vol. 1, No. 3.
- Xue H, *Privacy and personal data protection in China: An update for the year end 2009*, Computer Law & Security Review, 26 (2010) 284–289.
- Zhu G, *The Right to Privacy: An Emerging Right in Chinese Law*, Statute Law Review, Volume 18, Number 3, 1997, 208-214.

CAT: QA-01-15-844-EN-C (paper)
CAT: QA-01-15-844-EN-N (pdf)

DIRECTORATE-GENERAL FOR INTERNAL POLICIES

POLICY DEPARTMENT C
CITIZENS' RIGHTS AND CONSTITUTIONAL AFFAIRS

Role

Policy departments are research units that provide specialised advice to committees, inter-parliamentary delegations and other parliamentary bodies.

Policy Areas

- Constitutional Affairs
- Justice, Freedom and Security
- Gender Equality
- Legal and Parliamentary Affairs
- Petitions

Documents

Visit the European Parliament website:
http://www.europarl.europa.eu/supporting-analyses

PHOTO CREDIT: iStock International Inc.

ISBN 978-92-823-8355-1 (paper)
ISBN 978-92-823-8354-4 (pdf)

doi: 10.2861/234935 (paper)
doi: 10.2861/625170 (pdf)

Publications Office