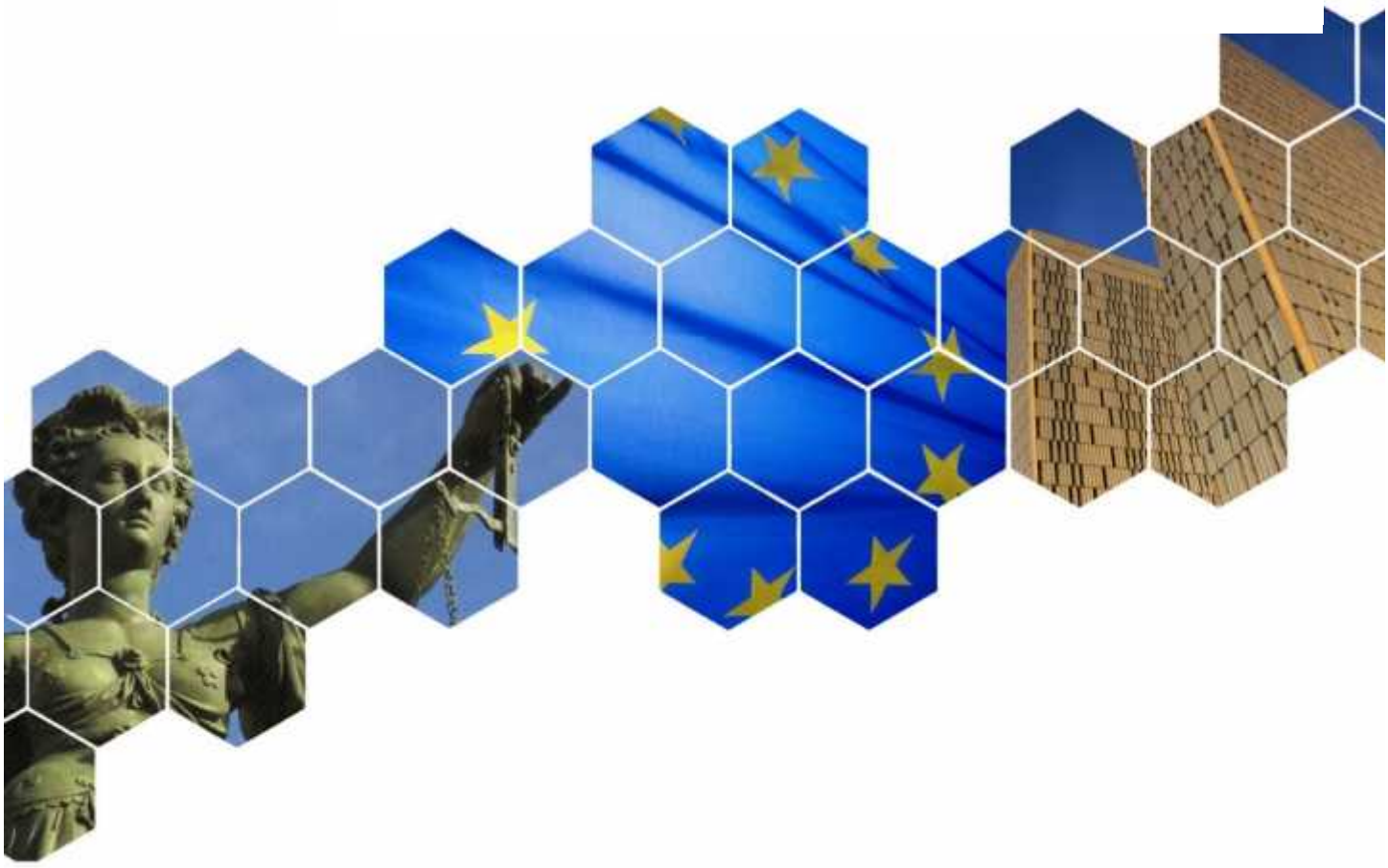
Government access to data in third countries

Final Report

EDPS/2019/02-13



milieu

KU LEUVEN

November 2021

This study has been prepared by Milieu under Contract No EDPS/2019/02-13 for the benefit of the European Data Protection Board (EDPB).

The study has been carried out by researchers from the Centre for IT and IP Law of KU Leuven with support from Milieu. The authors of the study are [redacted], Jan Czarnocki, Flavia Giglio, [redacted], Eyup Kun, Mykyta Petik and Dr Sofie Royer.

Milieu Consulting SRL, Chaussée de Charleroi 112, B-1060 Brussels, tel.: +32 2 506 1000; e-mail: EDPB.legalstudies@milieu.be ; web address: www.milieu.be.

TABLE OF CONTENTS

EXECUTIVE SUMMARY

The present report is part of a study analysing the implications for the work of the European Union (EU) / European Economic Area (EEA) data protection supervisory authorities (SAs) in relation to transfers of personal data to third countries after the Court of Justice of the European Union (CJEU) judgment C-311/18 on *Data Protection Commissioner v. Facebook Ireland Ltd, Maximilian Schrems* (Schrems II)[1]. Data controllers and processors may transfer personal data to third countries or international organisations only if the controller or processor has provided appropriate safeguards, and on the condition that enforceable data subject rights and effective legal remedies for data subjects are available. Whereas it is the primary responsibility of data exporters and data importers to assess that the legislation of the country of destination enables the data importer to comply with any of the appropriate safeguards, SAs will play a key role when issuing further decisions on transfers to third countries. Hence, this report provides the European Data Protection Board (EDPB) and the SAs in the EEA/EU with information on the legislation and practice in China, India and Russia on their governments' access to personal data processed by economic operators. The report contains an overview of the relevant information in order for the SAs to assess whether and to what extent legislation and practices in the abovementioned countries imply massive and/or indiscriminate access to personal data processed by economic operators.

For this study, a literature review via desk research (books, journal articles, databases and other online sources) was conducted as the primary step, in order to identify the relevant legal instruments and case law. Reports of international organisations were also compiled at this stage. After conducting a legal analysis of the collected sources, the loopholes in the knowledge in this area of law were defined for each country (India, China and Russia). Thereafter, a customised questionnaire was composed per country, tackling the higher defined loopholes. These country questionnaires were approved by the EDPB, making it possible to distribute the questionnaires to carefully selected experts in each country. To have a broad perspective, the researchers of this study strived to find persons working in different legal fields (academia, non-profit sector, the Bar ...). In total, 29 experts were contacted. However, only eight experts agreed to be interviewed. Reasons for refusal included lack of time and unwillingness to commit to the signature of additional documents, such as the consent form for data processing and non-disclosure agreement. The contacted experts responding positively to the invitation to participate in the questionnaire were subsequently interviewed. These interviews were conducted, both in writing and orally depending on the preference of the experts. As a last step for this study, the interviews were carefully analysed and compared with the results of the desk research. Where needed, anomalies were indicated. Based on this, the end report of the in-depth analysis of the countries was drafted including the results of the interviews.

The country report on the People's Republic of China (PRC) gives context to the Chinese legal system. It is held that the PRC is not a democratic, liberal state, nor does it have a rule of law. Therefore, it cannot be considered as having the ability to provide people with the protection of personal data equivalent to the EU. The report analyses and comments on basic Constitutional rules of the PRC and subsequently analyses secondary norms, regulating personal data processing, focusing on the processing of the personal data of foreigners by the government. It is argued that Chinese secondary laws should be interpreted with an eye on China's political system and Constitution. Analysis of both the Constitution of the PRC and secondary laws indicates that substantial protection of personal data against government access does not exist in the PRC. The Personal Information Protection Law (PIPL), which is the country's first comprehensive personal data protection legislation, is also discussed. It can be concluded that government access to personal data is not constrained. Several secondary laws concerning national security and the public order foresee exemptions to privacy protection legislations. The notions of security and the public order are given a wide interpretation and are considered priorities for the political system of the PRC. It can be argued that the PIPL and Data Security Law (DSL) do not pose significant limits to what the PRC government will be able to do with the peoples' data.

[1] CJEU 16 July 2020, C-311/18, *Schrems II*.

The country report on India starts off by giving an overview of the current state of the right of privacy and the right of data protection, considering the international treaties India is part of, and relevant judicial decisions impacting on the recognition of the right to privacy. The view of international human rights' organisations on the state of data protection in India is briefly analysed. After careful assessment of relevant Indian legislation, the purposes and conditions for governmental access to personal data are mapped out. Although in theory, oversight mechanisms are in place, these are not transparent in practice. Afterwards, the report provides information on the conditions for individuals to receive a remedy when their privacy rights are breached. It is striking that the Indian government cannot be held responsible for any data breaches. Lastly, the report provides an overview on the future developments of Indian legislation. Here, the features of the proposed Personal Data Protection (PDP) Bill are discussed. The report concludes that, while the right to privacy was recently recognised by the Supreme Court of India, the government still benefits from wide exemptions to the data protection regime for governmental access to personal data. The concept of 'national security' is recurring, vague and broad, and it is often used as a ground to access any personal information stored in the Indian territory, including personal data of persons in the EU. Although the Indian Supreme Court's Puttaswamy judgment confirmed that the constitutional right to privacy is part of a 'democratic order governed by the rule of law', including government access to data, data subjects' rights are quite limited, as well as the access to a redress mechanism in case of an infringement of the government. The same broad exemptions to data protection in the context of governmental access will be included in the DPD Bill as well.

The country report on Russia looks into the complex matter of Russian Personal Data Law. Whereas the right to privacy and data protection are both recognised in the Russian Constitution, their scope diverges from the corresponding EU rights. It can be noted that the Russian data access regime lacks specific and transparent criteria, and is far-reaching. In addition, the report looks into the several exemptions to data protection for government access to personal data. In light of this, the Federal Security Service is discussed. Further, national security and counter-terrorism has been limiting data subject rights. The country report notes that, considering the lack of transparency and judicial independence in such cases, intelligence and counter-intelligence agencies are virtually unrestricted in accessing data subjects' personal data. With regard to the different oversight mechanisms available, it can be held that there are concerns in terms of lack of judicial independence. Finally, the report illustrates the plans for a future federal database containing personal data of all Russian citizens. It can be concluded that, while the legislative framework seems comprehensive, the enforcement and application of the legislation shows the weaknesses of data protection in Russia. The right to privacy is strongly limited when interests of national security are at stake. The report argues that the law is used as an instrument to enforce political aspirations, resulting in legitimisation of new types of surveillance and censorship to control the flow of information in the country. The attitude towards the right to privacy is in line with a striking record of violating the European Convention of Human Rights, also in relation to other fundamental rights.

In the annexes included to this study, you will find the exact questionnaires per country (Annex 1), a list of all the used sources (Annex 2) and an overview of the used acronyms and abbreviations (Annex 3).

1 INTRODUCTION

1.1 OBJECTIVES AND SCOPE OF THE STUDY

The present report is part of a study analysing the implications for the work of the European Union (EU) / European Economic Area (EEA) data protection supervisory authorities (SAs) in relation to transfers of personal data to third countries after the Court of Justice of the European Union (CJEU) judgment C-311/18 on *Data Protection Commissioner v. Facebook Ireland Ltd, Maximilian Schrems* (Schrems II)[2]. According to Article 46 of the General Data Protection Regulation (GDPR)[3], data controllers and processors may transfer personal data to third countries or international organisations only if the controller or processor has provided appropriate safeguards, and on the condition that enforceable data subject rights and effective legal remedies for data subjects are available. Whereas it is the primary responsibility of data exporters and data importers to assess that the legislation of the country of destination enables the data importer to comply with any of the appropriate safeguards, SAs play a key role when issuing further decisions on transfers to third countries. Hence, this report provides the European Data Protection Board (EDPB) and the SAs in the EEA/EU with information on the legislation and practice in China, India and Russia on their governments' access to personal data processed by economic operators. The report contains an overview of the relevant information in order for the SAs to assess whether and to what extent legislation and practices in the abovementioned countries imply massive and/or indiscriminate access to personal data processed by economic operators.

As regards the specific research questions of the study, it is meant to firstly investigate the general situation of China, India and Russia concerning fundamental rights and freedoms, by analysing international reports and findings from public bodies (e.g. Council of Europe, UN Human Rights Council and Human Rights Committee) and renowned non-governmental bodies (e.g. Amnesty International, Human Rights Watch, Privacy International). To this end, the study also identifies the countries' international commitments in the field of human rights, in particular of the right to privacy and data protection. Secondly, the study analyses the legislation of the countries in order to establish the substantive and procedural conditions for government access to personal data, including law enforcement and intelligence agencies. Specific attention is given to the authorities involved in the adoption or amendment of the related rules, and entitled to authorise the governmental access to personal information. Afterwards, the study aims to investigate whether specific purposes and conditions to access personal data of foreign individuals exist in each of the three countries. The study also aims to identify, where existing, oversight mechanisms on the governmental access to personal data, and to assess the independency from the executive of the bodies empowered to perform such control. Finally, the study focuses on which rights and administrative or judicial redress mechanisms are available to data subjects (including foreigner individuals) in the three observed countries.

1.2 LEGAL BACKGROUND

Governmental access to personal data does not only affect the right to protection of personal data (Article 8 of the Charter of Fundamental Rights of the European Union - EU-Charter[4]), but also more broadly the right to respect of private life (article 7 EU-Charter) and even the right to freedom of expression and information (Article 11 EU-Charter)[5]. When someone feels that their private lives are the subject of

[2] CJEU 16 July 2020, C-311/18, *Schrems II*.
[3] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).
[4] Charter of Fundamental Rights of the European Union, OJ C 326, 26.10.2012, p. 391–40, viewed 6 September 2021, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:12012P/TXT.
[5] CJEU 8 April 2014, C-293/12 and C-594/12, *Digital Rights*, §25,70; CJEU 21 December 2016, C-203/15 and C-698/15, *Tele2 Sverige*, §93.

constant surveillance, it can cause nervousness[6]. Nevertheless, the aforementioned fundamental rights are not absolute. They can be restricted if limitations are (i) provided by law; (ii) necessary to meet objectives of general interest recognised by the EU; and (iii) proportionate (Article 52 EU-Charter)[7]. In doing so, the essence of the fundamental rights may never be compromised[8]. On a privacy regulation level, the e-Privacy Directive[9] and the GDPR[10] are relevant in case of data transfers[11]. In particular Article 23 of the GDPR mirrors the requirements of Article 52 of the EU-Charter and needs to be read in light of the EU-Charter. In that regard, it is also important to refer to Article 44 of the GDPR, which states that the level of protection in a third country must be essentially equivalent to the level of protection within the EU[12]. This means that these data transfers need to comply with the GDPR and the e-Privacy Directive[13] and that these provisions must be interpreted in light of the EU Charter[14]. Whereas both the GDPR and the EU-Charter describe those requirements in a rather broad wording, further guidance can be found in the case law of the CJEU and the European Court of Human Rights (ECtHR)[15]. The criteria developed by these Courts are mentioned below, allowing the reader to keep them at the back of his or her mind when going through the analysis of the third country in section 2.

1.2.1 Legality

First, limitations of fundamental rights need to have a legal basis in national legislation. Article 23(2) GDPR states the elements that should be legally defined in case of a restriction of the protection of personal data (i.e. the scope, the safeguards to prevent abuse or unlawful access, the storage period, the right of a data subject to be informed about the restriction…)[16]. Again, the GDPR is not directly applicable in third countries and the legal situation will be assessed by supervisory authorities. However, it is still relevant to look into the requirements of the GDPR, as a starting point.

In its case law, the CJEU generally states that the legislation permitting the interference must define the scope of the limitation on the exercise of the rights concerned[17]. Also, the interfering measures always need to be foreseeable[18]. The definition of foreseeability under the quality of law requirement is well established in the case law of the ECtHR[19]. In a landmark decision of 25 May 2021, the ECtHR clarified

[6] *Digital Rights*, §27 and §37; *Tele2*, §99-100.
[7] EDPB, *Recommendations 02/2020 on the surveillance measures*, 10 November 2020, p. 10.
[8] CJEU 26 July 2017, *Opinion 1/15 on the EU-Canada PNR Agreement*, §124, §138-141, §150; EDPB, *Guidelines 10/2020 on restrictions under Article 23 GDPR*, 15 December 2020, p. 6.
[9] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications' sector (Directive on privacy and electronic communications).
[10] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).
[11] After all, in *Schrems II*, the CJEU made clear that the GDPR as a whole remains applicable even if these data will be processed by the third country by the time of transfer or thereafter for the purposes of public security, defence and State security. See also: CJEU 6 October 2015, C-362/14, *Schrems I*; CJEU 16 July 2020, C-311/18, *Schrems* II §86-88; CJEU 20 October 2020, C-623/27, *Privacy International*, §35, §39, §44 and §49.
[12] *Schrems I*, §64; *Schrems II*, §105, §188.
[13] *Schrems I*, §64; *Schrems II*, §105, §188.
[14] *Schrems II*, §105.
[15] The interpretation of the ECtHR is also relevant, because the meaning and scope of the rights in the EU-Charter shall be (at least) the same as the corresponding rights in the European Convention of Human Rights (ECHR). See Article 52 (3) EU-Charter.
[16] Such elements are: (a) the purposes of the processing or categories of processing; (b) the categories of personal data; (c) the scope of the restrictions introduced; (d) the safeguards to prevent abuse or unlawful access or transfer; (e) the specification of the controller or categories of controllers; (f) the storage periods and the applicable safeguards taking into account the nature, scope and purposes of the processing or categories of processing; (g) the risks to the rights and freedoms of data subjects; and (h) the right of data subjects to be informed about the restriction, unless that may be prejudicial to the purpose of the restriction. See also EDPB, *Guidelines 10/2020 on restrictions under Article 23 GDPR*, 15 December 2020.
[17] *Schrems II*, §175; *Privacy International*, §65.
[18] EDPB, *Guidelines 10/2020 on restrictions under Article 23 GDPR*, 15 December 2020, 6-7.
[19] ECtHR 4 December 2015, no. 47143/06, *Zakharov v. Russia*, §228-230.

this principle further in relation to government surveillance measures and bulk interception of communication[20]. It held that the following minimum requirements should be set out in law: (i) nature of offences which may give rise to a limitation; (ii) a definition of the categories of people liable to have their communications intercepted; (iii) a limit on the duration of interception; (iv) the procedure to be followed for examining, using and storing the data obtained; (v) the precautions to be taken when communicating the data to other parties and the circumstances in which intercepted data may or must be erased or destroyed[21].

1.2.2 Objectives of general interest

Next, limitations need to be strictly necessary to obtain an objective mentioned by the EU Legislation or the need to protect the rights and freedoms of others. Article 3 of the Treaty on European Union, for instance, mentions freedom, security and justice as general objectives[22]. Article 23 of the GDPR, in its turn, states that data protection can be limited for the purposes of security, defence and state security[23]. In that regard, the case law of the CJEU in data retention is worth mentioning. In the past, legislation in several Member States made it possible to retain data in a general and indiscriminate manner for the purposes of national security, public security and the combat of crime. The expiration date of general data retention for the purpose of the combat of crime has elapsed, as the CJEU repeatedly declared many of those national legislations invalid. Whereas such data retention exceeds the limits of what is strictly necessary in a democratic society according to the CJEU, limited exceptions can be envisaged, both in cases of national security and the combat of serious crime[24].

1.2.3 Proportionality

Finally, a balance needs to be struck between the means used and the intended aim[25]. The proportionality requirement applies to data retention, data access, data use, data collection and other processing, and may differ depending on type of data and type of objective. In what follows, we give some examples on the proportionality requirement of the case law on data retention of the CJEU[26]. In its proportionality assessment, the Court differentiates first between general and targeted data retention, the latter being less invasive. Second, threats to national security can justify more invasive limitations than the fight against (serious) crime or safeguarding public security[27] (from serious threats). Third, the CJEU differentiates between different kinds of (communication) data. Content data can never be retained[28]. The Court considers the retention of data relating to civil identity[29] as, in principle, less serious than the

[20] ECtHR 25 May 2021, nr. 58170/13, 62322/14 and 24960/15, *Big Brother Watch and Others/The United Kingdom* (§361); E. Watt, "Much Ado About Mass Surveillance – the ECtHR Grand Chamber 'Opens the Gates of an Electronic "Big Brother" in Europe' in Big Brother Watch v UK", *Strasbourg Observers* viewed 28 June 2021, https://strasbourgobservers.com/.
[21] *Big Brother Watch*, §335.
[22] EDPB, *Recommendations 02/2020 on the European Essential Guarantees for surveillance measures*, 10 November 2020, p. 11.
[23] See also EDPB, *Guidelines 10/2020 on restrictions under Article 23 GDPR*, 15 December 2020.
[24] CJEU 6 October 2020, C-511/18, C-512/18 and C-520/18, *La Quadrature du Net*, §100, §122, §136, §140-151; *Privacy International*, §45, §75.
[25] EDPB, *Recommendations 02/2020 on the European Essential Guarantees for surveillance measures*, 10 November 2020, p. 10; European Data Protection Supervisor (EDPS), *Case Law Digest: Transfers of personal data to third countries*, 10 June 2021.
[26] See for a more thorough overview: EDPS, *Guidelines on assessing the proportionality of measures that limit the fundamental rights to privacy and to the protection of personal data*, 19 December 2019.
[27] *Privacy International*, §135-136.
[28] Tracol, X. (2019). Ministerio fiscal: Access of public authorities to personal data retained by providers of electronic communications services. European Data Protection Law Review (EDPL), vol. 5(1), pp. 127-135.
[29] Data related to civil identity can be defined as data providing contact information (e.g. name, postal address…). See *La Quadrature du Net*, §157.

retention of traffic[30] and location[31] data[32]. As a consequence, Member States are allowed to conduct a general retention on data relating to civil identity for the purposes of combating crime in general and for safeguarding public security[33]. In light of combating serious crime, preventing serious threats to public security and safeguarding national security, targeted preventive retention of traffic and location data is possible if certain requirements are met[34]. In practice, that retention must always be limited with respect to the categories of data to be retained[35], the retention period (which should be limited but can be renewed[36]), the means of communication affected, and the persons concerned[37]. In light of the last requirement, retention should be based on objective evidence for targeting people, revealing a (indirect) link to the purpose in question[38]. In doing so, a geographical criterion for determining limits of the retention can be adopted: areas with high incidence of serious crime are particularly vulnerable: infrastructures and places with very high volume of visitors, strategic locations… (airports etc.)[39]. All these elements must be adopted in binding legislation[40]. A general and indiscriminate data retention of traffic and location data for a limited period of time, however, is only allowed when a threat to national security proved to be genuine, present and foreseeable[41].

The proportionality assessment extends to the access to and the use of retained data, which should also be limited to what is strictly necessary for the purpose of the investigation[42]. Authorisation must be asked prior to the access to the data (except in the event of a justified urgence)[43]. This review needs to be carried out either by a court or by an independent administrative body whose decision is binding[44]. Lastly, it is also of great importance that adequate safeguards preventing abuse are adopted[45]. This entails that effective judicial and administrative redress should be in place[46]. Furthermore, data subjects need to have an effective possibility to have access to the retained data, to obtain rectification or to erase data[47]. Finally, in case of a restriction of the right to the protection of personal data, the CJEU stresses on notifying the persons whose data has been accessed, as soon as that notification is no longer liable to jeopardise ongoing (criminal) investigations[48]. The ECtHR also takes a notification into account as a relevant factor in assessing the effectiveness of remedies before the courts and hence to the existence of effective safeguards against the abuse of surveillance powers[49].

1.3 STUDY METHODOLOGY

For this study, a literature review via desk research (books, journal articles, databases and other online sources) was conducted as the primary step. The purpose of this review was to map the law in the books, consisting of the relevant legal instruments and relevant case law. In addition, reports of international

[30] Traffic data can be defined as data processed for the purpose of the conveyance of a communication on an electronic communications network or for the billing thereof (Article 2(b) e-Privacy Directive).
[31] Location data is any data processed in an electronic communications network, indicating the geographic position of the terminal equipment of a user of a publicly available electronic communications service (Article 2(c) e-Privacy Directive).
[32] *La Quadrature du Net*, §157.
[33] *La Quadrature du Net*, §158.
[34] *Tele2*, §108; *La Quadrature du Net*, §140, §147; CJEU 2 March 2021, C-746/18, *Prokuratuur*, §35.
[35] *La Quadrature du Net*, §147-151.
[36] *La Quadrature du Net*, §137-139, § 163; *Big Brother Watch*, §335.
[37] *Tele2*, §110; *La Quadrature du Net*, §147-151.
[38] *Tele2*, §110; *La Quadrature du Net*, §147-151.
[39] *Tele2*, §109-111; *La Quadrature du Net* §147-151.
[40] *La Quadrature du Net*, §132-133; *Prokuratuur*, §48-50.
[41] *La Quadrature du Net*, §107-108, §136- 137; *Privacy International*, §81.
[42] *Prokuratuur*, §38.
[43] *Tele2*, §120; *La Quadrature du Net*, §137-139; *Prokuratuur*, §40, §53-54, §58; *Big Brother Watch*, §355.
[44] *Tele2*, §120; *Prokuratuur*, §53-54.
[45] *Opinion 1/15 on the EU-Canada PNR Agreement*, §57, §219, §226.
[46] *Opinion 1/15 on the EU-Canada PNR Agreement*, §57, §219, §226.
[47] *Opinion 1/15 on the EU-Canada PNR Agreement*, §220; *La Quadrature du Net*, §190.
[48] *Tele2*, §121.
[49] However, it does not make it mandatory if the domestic remedies permit any person who suspects that his or her communications are being or have been intercepted to apply to the courts. *Big Brother Watch*, §357-358.

organisations were compiled in this step. After conducting a legal analysis of the collected sources, the loopholes in the knowledge in this area of law were defined for each country (India, China and Russia). Thereafter, focus was laid on the law in action. Per country, a customised questionnaire was composed, tackling the higher defined loopholes. These country questionnaires were approved by the EDPB, making it possible to distribute the questionnaires to carefully selected experts in each country. At least three experts were detected per country. To have a broad perspective, the researchers of this study strived to find persons working in different legal fields (academia, non-profit sector, the Bar...).

For China, nine experts were contacted, resulting in two positive responses, two negative answers and five who did not reply. For India, eleven experts were contacted, resulting in five positive responses, one negative reply and five who did not reply. Whereas five experts completed the NDA and consent form, only one expert took part in the interviews in the end. For Russia, nine experts were contacted, resulting in one positive response. A frequent reason used for not participating in the study was lack of time and unwillingness to formalise the interview by signing the additional documents such as the consent form to data processing and non-disclosure agreement. However, in most cases, the authors of this study simply did not receive an answer or the negative response did not contain any explanation as to why the contacted expert was not able to participate in the study. Based on these responses, the external experts were interviewed via country specific questionnaires (see Annex 1). These interviews were conducted, both in writing and orally depending on the preference of the experts. As a last step for this study, the interviews were carefully analysed and compared with the results of the desk research. Where needed, anomalies were indicated. Based on this, the end report of the in-depth analysis of the countries was drafted including the results of the interviews.

1.4 STRUCTURE OF THIS REPORT

Section 2 describes an in-depth analysis of the legislation and practice on government access to personal data in China (Section 2.1), India (Section 2.2) and Russia (Section 2.3). The same structure is followed in every country section.

Each country section presents a first subsection aimed to answer the research question concerning the general situation of the countries as regards human rights, and specifically the right to privacy and data protection. It provides an overview concerning rule of law, respect for human rights and fundamental freedoms in the observed countries. The main constitutional provisions of each of the countries are analysed, as well as the concrete application of such provisions in the national case law. The subsection also illustrates whether and how the right to privacy exists in each of the three legal systems. Afterwards, the general findings by international organisations on the three countries' human rights situation are also briefly shown.

Subsequently, the country reports include a subsection illustrating the purposes, conditions, and oversight mechanisms of the governmental access to personal data in each of the three countries. This subsection aims to answer the research questions related to the specific legislative requirements for government access to personal data; where specific provisions on foreign individuals' personal data do not always exist in the three legal systems, the report also tries to address the research questions around the applicability of the countries' legislation to foreigners.

In each country section, a subsection is dedicated to the data subjects' rights, their conditions for applicability and the redress mechanisms available to enforce them. The subsection's goal is to answer the research questions around individual rights and existing redress mechanisms as regards the right to privacy in the legal systems of the three countries.

Finally, a subsection is dedicated in each country section to provide an overview of the upcoming changes in the legislation on government access to personal data: the goal is to offer an overview on how the legal systems of the three countries are likely to evolve in relation to the right to privacy and

data protection in the near future.

Section 3 provides conclusions by answering the research questions.

The annexes included to this study entail exact questionnaires per country (Annex 1), a list of all the used sources (Annex 2) and an overview of the used acronyms and abbreviations (Annex 3).

2 IN-DEPTH ANALYSIS OF THIRD COUNTRIES

The following section aims to answer the research questions of the study in relation to the three countries. The structure of the subsections is consistent with a division into areas of interests touched upon by the research questions. The answers are integrated in the related subsections. Each section provides an in-depth analysis of the legislation and practice in third countries on their governments' access to personal data. Section 2.1 deals with the situation in China, Section 2.2 with India and Section 2.3 with Russia. All these sections study the situation in third countries from the perspective of the rule of law and respect for human rights and fundamental freedoms; government access to personal data; and data subject rights. Moreover, any potential upcoming changes in the legislation are also discussed. Finally, every country section contains an intermediary conclusion and a grid visually presenting the research results.

2.1 CHINA

2.1.1 Rule of law, respect for human rights and fundamental freedoms

2.1.1.1 Context

While analysing the legal system of the People's Republic of China (PRC), the following assumptions embedded in the Western legal system do not apply[50]. The first assumption, is the existence of a legality principle, which is the notion that law regulates and constrains the behaviour of public authorities. Consequently, the second assumption is that the access of the government to personal data can be limited by law in China. Thus, the third assumption is that people in China would have rights against the government. Further, that citizens of China can object to decisions of the government, or have legal remedies, through which they can claim their rights. The final assumption entails the idea that there is a separation of powers, meaning that an independent judicial branch exists, controlling and restraining governmental access to data. These assumptions about law are not applicable in China and need to be left out to properly understand Chinese law. A different understanding of the law and its role in the PRC is required—compared to the Western legal tradition.

Looking at the international commitments of the PRC, it can be held that the International Covenant on Civil and Political Rights (ICCPR) was signed in 1998[51], but has not been ratified up to now[52]. This is of relevance as Article 17 of the ICCPR ensures the right to privacy to anyone.

First of all, according to Article 1 of the Constitution of the PRC[53], China is a socialist state under a democratic dictatorship, led by the Communist Party of China (CCP)[54]. Constitutional changes after the Second World War led to the structural unification of the Chinese Communist Party and state, resulting in the CCP's dominance over the state's normative system[55]. This system interprets the rule of law as

[50] Von Blomberg, M., 2018, 'The Social Credit System And China's Rule Of Law', Mapping China Journal, pp.77-162, viewed 21 July 2021.
[51] Article 17 of this UN treaty ensures the right to privacy to anyone.
[52] For other UN Treaties that China signed, see https://tbinternet.ohchr.org/_layouts/15/TreatyBodyExternal/Treaty.aspx?CountryID=36&Lang=E.
[53] Article 1 of the PRC Constitution 2017, http://english.www.gov.cn/archive/lawsregulations/201911/20/content_WS5ed8856ec6d0b3f0e9499913.html, viewed 21 July 2021.
[54] *Ibid.*; For the report on the party-state's tech-enhanced authoritarianism, Hoffman, S., 2019, 'Engineering global consent: The Chinese Communist Party's data-driven power expansion', https://www.aspi.org.au/report/engineering-global-consent-chinese-communist-partys-data-driven-power-expansion, viewed 27 July 2021.
[55] LI, L., 2015, 'Rule of Law' in a Party-State: A Conceptual Interpretive Framework of the Constitutional Reality of China', 2 Asian Journal of Law and Society, 93. viewed 21 July 2021.

rule by law under the Rule of the Party[56]. According to Article 3 of the Constitution, China is ruled according to the principle of democratic centralism, which entails concentration of power in the people's congresses and an absence of a separation of power safeguarded by a system of checks and balances. Further, according to Article 5 of the Constitution, the PRC rules the country according to law and establishes it as a socialist state governed by law. All power, including judicial and law enforcement, is concentrated in the National People's Congress (NPC), which supervises other state organs. The NPC is at the same time the legislative, executive, and judicial branch of the government, meaning that there is no separation of power. The NPC is directly supervised by the government and the CCP, and realises their policies[57]. Most of the judges in the PRC's judicial system are appointed by local party leaders, hence the judiciary is not independent[58]. For this reason, the rule of law in China generally has been described as the rule of law with Chinese characteristics[59]. Based on the lack of separation of powers, the supremacy of law, legal certainty, and judicial independence, China's legal system cannot be defined as being a liberal democratic system and being a rule of law system by Western standards[60].

Chapter II of the Constitution covers the fundamental rights and obligations of the citizens. Article 33(1) of the Constitution defines the notion of citizenship by stating that "*all people holding the nationality of the People's Republic of China are citizens of the PRC*". Article 33(4) further states that "*every citizen shall enjoy the rights prescribed by the Constitution and the law*". There is thus a direct link between citizenship and human rights. Article 40 provides that freedom and confidentiality of correspondence of citizens shall be protected by law.

Irrespective of Article 40, however, the entire basis for Chinese privacy law assumes that community stability should prevail over the needs of individual persons[61]. When it comes to processing of personal data, therefore, numerous exceptions are made for national security or criminal investigations where they are needed, with no further restrictions on how these exceptions should be interpreted. According to Article 50 of the Constitution, the rights of the citizens cannot impede the interest of the state and society[62]. Reading this Article in conjunction with Articles 1 and 3 leads to the conclusion that the CCP defines the collective interests of the state. In other words, the CCP decides to what extent and how the individual's rights can be exercised.

As there is a direct reference to the citizens in Chapter II of the Constitution, it can be argued that these rights are only provided to the citizens of China. Article 32 of the Constitution, which does not fall within the scope of Chapter II, confirms this argument. It states that the PRC protects the lawful rights and interests of foreigners in the territory of China, thereby limiting the scope of the protection extended to foreigners compared to Chinese citizens. On the other hand, there are arguments for stating that the constitutional protection for foreigners and citizens is the same[63]. This argument has several bases. In different procedural laws, such as in administrative proceedings, foreigners, stateless people, and foreign

[56] *Ibid.*
[57] Zhizheng, W., 2012, 'Systematic government access to private-sector data in China, International Data Privacy Law, Volume 2, Issue 4, pp. 220–229, viewed 21 July 2021.
[58] According to the interview with an expert.
[59] Castellucci, I., 2007, 'Rule of Law with Chinese Characteristics', Annual Survey of International & Comparative Law, vol. 1, no. 1, pp 35-92 http://digitalcommons.law.ggu.edu/annlsurvey/vol13/iss1/4; See for instance, the relationship between rule of law and social credit core practices in China, Creemers, R., 2018, 'China's Social Credit System: An Evolving Practice of Control', viewed 21 July 2021, https://ssrn.com/abstract=3175792.
[60] Burnay, M., 2016, 'Bridging the EU-China's Gap on the Rule of Law?', Asia Europe Journal, vol. 14, no. 1, pp. 95–106, 101; Ruskola, T., 2003, 'Law without law, or is Chinese law an oxymoron', William & Mary Bill of Rights Journal 11(2), pp. 655-670; See for the discussion on socialist rule of law with Chinese Characteristics, Moritz, R., 2021, 'Xi Jinping Thought on the Rule of Law', viewed 27 July 2021, https://www.swp-berlin.org/publications/products/comments/2021C28_Jinping_RuleOfLaw.pdf.
[61] Li, T. and Bronfman, J. and Zhou, Z., 2017, 'Saving Face: Unfolding the Screen of Chinese Privacy Law' (August 2017). Journal of Law, Information, and Science (Forthcoming), pp. 1-33, p. 12, viewed 28 July 2021, https://ssrn.com/abstract=2826087.
[62] Article 50 of the PRC Constitution 2017, viewed 21 July 2021.
[63] According to the interview with an expert.

organisations have the same rights and obligations as Chinese citizens. In terms of government data access, there is no distinction between foreign nationals and Chinese citizens. However, as no such legal case has been reported in practice, hypothetical conclusions cannot be drawn in the absence of actual case-law[64]. Even though this argument would comply with Article 32 of the Constitution with respect to foreigners residing on the territory of the PRC, the extent to which foreigners residing outside of China are equally protected by the Constitution is unclear. Nevertheless, it can be stated that the constitutional rights under the Chinese legal system will in any case rarely be subject to administrative litigation[65], thus the protection bestowed by the Constitution itself might not make a meaningful difference between Chinese citizens and foreigners, irrespective of where they reside.

As of 1 November 2021, China has a general data protection regime. The country's first – and long-awaited – comprehensive personal data protection legislation, the Personal Information Protection Law (PIPL), was adopted on 20 August 2021. This Act comprehensively covers the protection of personal information, including the 'full lifecycle' of personal information[66]. Before this Law entered into force, there were more than 100 regulations concerning the protection of personal information. The overall structure is considered to be ineffective in terms of ensuring legal rights for individuals due to complexity and dispersion of these regulations. The impact of this law will be discussed further in section 2.1.4.

One of the most comprehensive legislations is the Cybersecurity Law (CSL). Article 1 of the CSL emphasises cyberspace sovereignty, national security, social and public interest to protect "*lawful rights and interests of citizens*". The primary goal of this law is to seek national security[67]. Another important legislation in terms of privacy and data protection is the Civil Code. This law was promulgated in 2020 and took effect on 1 January 2021[68]. It bestows numerous rights such as the prohibition to process personal data without consent[69], the prohibition of excessive processing[70], and the obligation to process personal data in compliance with the principles of lawfulness, justification, and within a necessary time frame[71].

At face value, rights and obligations related to the right on data protection are similar to those introduced by the GDPR. Although Western concepts seem to be implemented, this is only the case as to their form, not as to their intended effects, especially in relation to government access[72]. Finally, it can be mentioned that, even though there is a clear tendency to strengthen personal data protection in the private sector, there are no specific restrictions on government access to personal data (see section 2.1.2: Government access to personal data).

[64] *Ibid.*
[65] *Ibid.*
[66] Huang, Y. and Mingli S., 'Top Scholar Zhou Hanhua Illuminates 15+ Years of History Behind China's Personal Information Protection Law', viewed 23 August 2021, https://digichina.stanford.edu/news/top-scholar-zhou-hanhua-illuminates-15-years-history-behind-chinas-personal-information.
[67] Qi, A. and Guosong, S. and Wentong, Z., 2018, 'Assessing China's Cybersecurity Law', Computer Law & Security Review Volume 34, Issue 6, pp. 1342-1354, viewed 28 July 2021, https://www.sciencedirect.com/science/article/abs/pii/S0267364918303157.
[68] Civil Code of the PRC, viewed 28 July 2021, http://english.www.gov.cn/archive/lawsregulations/202012/31/content_WS5fedad98c6d0f72576943005.html.
[69] Article 1032 and 1033 of Civil Code of the PRC, viewed 28 July 2021, http://english.www.gov.cn/archive/lawsregulations/202012/31/content_WS5fedad98c6d0f72576943005.html.
[70] Article 1035 Civil Code of the PRC, viewed 28 July 2021, http://english.www.gov.cn/archive/lawsregulations/202012/31/content_WS5fedad98c6d0f72576943005.html.
[71] *Ibid.*
[72] Pernot-Leplay, E., 2020, 'China's Approach on Data Privacy Law: A Third Way Between the U.S. and the E.U.?', PENN. ST. J.L. & INT'L AFF., vol. 8, no. 1, pp. 49-117, viewed 28 July 2021, https://elibrary.law.psu.edu/cgi/viewcontent.cgi?article=1244&context=jlia.

2.1.1.2 General findings of international organisations

According to numerous reports by international human rights' organisations, fundamental rights of people are notoriously abused in PRC[73]. In several reports, Human Rights Watch states that China does not meet international standards with respect to surveillance by different government authorities[74]. With regard to privacy and data protection, the surveillance enrolled in the province of Xinjiang can be an example of a deteriorating situation[75]. Chinese surveillance efforts and building of so called social-credit system and export of this model outside of its territory was labelled "digital authoritarianism"[76].

2.1.2 Government access to personal data

2.1.2.1 Purposes

i. General

According to Article 40 of the Constitution of the PRC, the freedom and privacy of its citizen's correspondence are protected by law. No organisation or individual may, under any circumstances, infringe that freedom and privacy, except where necessary to meet the needs of State security, or in cases where criminal investigation, public security or procuratorial organs are permitted to censor correspondence in accordance with legal procedures. Article 40 of the Constitution is the primary source of authorisation for public bodies to access personal data processed by private actors[77]. Since legislation on government access to personal data is dispersed and provides public security officials with broad discretion, the PRC's mass surveillance programmes go unchallenged in China[78]. It is generally argued that the Chinese government is said to have no restrictions when requesting companies to provide access to personal information. For example, no court orders are required. This demonstrates that government interests take precedence over constitutional rights[79]. Moreover, the Chinese party-state establishes mechanisms and power structures to ensure data access by government authorities domestically and

[73] Human Rights Watch, 2021, China's Crimes against Humanity Targeting Uyghurs and Other Turkic Muslims | HRW, https://www.hrw.org/report/2021/04/19/break-their-lineage-break-their-roots/chinas-crimes-against-humanity-targeting, viewed 8 August 2021, Human Rights Watch 2018, China's Campaign of Repression Against Xinjiang's Muslims | HRW, https://www.hrw.org/report/2018/09/09/eradicating-ideological-viruses/chinas-campaign-repression-against-xinjiangs, viewed 8 August 2021.

[74] Human Rights Watch, 2019, China's Algorithms of Repression Reverse Engineering a Xinjiang Police Mass Surveillance App, viewed 28 July 2021, https://www.hrw.org/report/2019/05/01/chinas-algorithms-repression/reverse-engineering-xinjiang-police-mass.

[75] Human Rights Watch, 2019, China's Algorithms of Repression Reverse Engineering a Xinjiang Police Mass Surveillance App, viewed 28 July 2021, https://www.hrw.org/report/2019/05/01/chinas-algorithms-repression/reverse-engineering-xinjiang-police-mass, Human Rights Watch, Detention and Torture in the Chinese Communist Party's Shuanggui System | HRW, viewed 8 August 2021, https://www.hrw.org/report/2016/12/06/special-measures/detention-and-torture-chinese-communist-partys-shuanggui-system, Amnesty International, Everything you need to know about human rights in China | Amnesty International | Amnesty International, viewed 13 September 2021, https://www.amnesty.org/en/countries/asia-and-the-pacific/china/report-china/.

[76] Lilkov, D, 2020, 'Made in China: Tackling Digital Authoritarianism', WMCES, Made in China: Tackling Digital Authoritarianism | Martens Centre, accessed 19 August 2021.

[77] Wang, Z., 2017, 'Systematic Government Access to Private-Sector Data in China' in Fred C. and Dempsey, J. (ed), '*Bulk Collection: Systematic Government Access to Private-Sector Data*, Oxford University Press, pp. 241-258, p. 241, viewed 28 July 2021, https://oxford.universitypressscholarship.com/view/10.1093/oso/9780190685515.001.0001/oso-9780190685515-chapter-11.

[78] Geller, A., 2020, 'How Comprehensive Is Chinese Data Protection Law? A Systematisation of Chinese Data Protection Law from a European Perspective', GRUR International, Volume 69, Issue 12, pp. 1191–1203, p. 1202, viewed 28 July 2021, https://academic.oup.com/grurint/article/69/12/1191/5909207.

[79] Pernot-Leplay, E., 2020, 'China's Approach on Data Privacy Law: A Third Way Between the U.S. and the E.U.?', PENN. ST. J.L. & INT'L AFF., vol. 8, no. 1, pp. 49-117, viewed 28 July 2021, https://elibrary.law.psu.edu/cgi/viewcontent.cgi?article=1244&context=jlia.

globally[80].

ii. Criminal investigations

There is no specific provision on the processing of personal data during criminal investigations. This can be considered one of the weaknesses of the current regulatory framework on electronic evidence[81]. According to Sections 5 and 6 of the Criminal Procedure Law, investigators can carry out the search and seizure procedure. As acquiring evidence is classified as an investigative activity under Chinese criminal procedure, only police officials have the authority to conduct such actions. Neither the judge nor the prosecutor will intervene in this process, giving investigators a lot of leeway, and perhaps jeopardising criminal suspects' right to know[82].

Furthermore, Article 6 of the Provisions on several issues concerning the collection, taking, examination, and the judgment of electronic data in the handling of criminal cases (Provisions 2016)[83] states that all data stored, both at Chinese territory and abroad, can be accessed online. This Article has caused considerable controversy, with many countries seeing it as a violation of cyberspace sovereignty[84].

As a result, it has been changed by Article 23 of the Rules of obtainment of electronic data as evidence by public security authorities in handling criminal cases promulgated by the Ministry of Public Security of the PRC in 2019 (Rules 2019)[85]. This Article states that investigators can collect electronic data online (including personal information) for criminal investigations. For data in the 'domestic distance computer information system', being a computer system located in China, all data can be collected[86]. In terms of electronic data stored abroad, *only* publicly available data can be accessed[87]. The online remote investigations are to be carried out by relevant case-handling public security authorities. For any case with significant facts and with a complicated crime scene, the higher-level public security authority can directly coordinate an online distance investigation as he/she considers this to be appropriate, according to Article 28 of the Rules 2019. In the case of a criminal investigation against foreign individuals, according to the rules mentioned above, electronic data, including personal data can be accessed by police officers.

iii. The Cybersecurity Law

The Cybersecurity Law of the PRC applies to network operators, i.e. network owners, managers, and network service providers (Article 76 of the Cybersecurity Law). This broad definition covers the entire network system, comprising computers or other information terminals and supporting equipment that adheres to specific rules and procedures for information gathering, storage, transmission, exchange, and processing (Article 76 of the Cybersecurity Law). According to Article 28 of the Cybersecurity Law, network operators must provide technical support and assistance to the public security and national

[80] Hoffman, S. and Attrill, N., 2021, 'Mapping China's Technology Giants: Supply chains and the global data collection ecosystem', viewed 28 July 2021, https://www.aspi.org.au/report/mapping-chinas-tech-giants-supply-chains-and-global-data-collection-ecosystem.

[81] Yang, F. and Feng, J., 2021, 'Rules of electronic data in criminal cases in China', International Journal of Law, Crime and Justice, Vol. 64, pp. 1-11, https://www.sciencedirect.com/science/article/pii/S1756061620304882#:~:text=The%20amendment%20to%20the%20Criminal,physical%20evidence%20nor%20documentary%20evidence.

[82] *Ibid* p. 9.

[83] *Ibid.*, These provisions are copied from this article.

[84] *Ibid.*

[85] Yang, F. and Feng, J., 2021, 'Rules of electronic data in criminal cases in China', International Journal of Law, Crime and Justice, Vol. 64, pp. 1-11, https://www.sciencedirect.com/science/article/pii/S1756061620304882#:~:text=The%20amendment%20to%20the%20Criminal,physical%20evidence%20nor%20documentary%20evidence.

[86] *Ibid*, p. 9.

[87] *Ibid.*

security organs that protect national security and investigate criminal activity in accordance with the law[88]. This provision does not stipulate any limitations or restrictions to the scope of this technical assistance[89]. Also, the criminal procedure law and national intelligence law do not foresee any restriction in this sense. In other words, the support and assistance given might include access to data and metadata content[90]. Article 69 of the Cybersecurity Law stipulates the imposition of monetary fines on both network operators and directly responsible management personnel for refusal to provide technical support and assistance to public security organs and state security organs. Network operators may therefore be motivated to provide the necessary information to comply with this provision.

The Cybersecurity Law imposes additional obligations on critical information infrastructure operators, which includes public communications and information services, and other infrastructure that may endanger national security (Article 31 of the Cybersecurity Law). Article 37 of the Cybersecurity Law stipulates that operators of critical information infrastructure that collect or generate personal information or important data while operating on the PRC mainland must keep it on the mainland. Where business requirements genuinely necessitate providing data outside the mainland, they shall follow the measures jointly formulated by the State cybersecurity and informatisation departments and the relevant State Council departments to conduct a security assessment. Where laws and administrative regulations provide otherwise, they shall follow those provisions.

As there is a data localisation requirement for operators of critical information infrastructure, this provision can extend the scope of information access by the government. Considering the broad power given to investigators in the criminal investigation process (see above), the data localisation requirement may have this impact. On the other hand, this provision covers handling of personal information for the critical information infrastructure operators in China and may not be considered an aggravating factor for government access to the personal data of natural persons living outside the PRC. This interpretation assumes that the obligation pertains to the protection of personal data of people residing in China and that those operators process the personal information of people in China.

iv. The National Security Law

Article 77 of the National Security Law of the PRC stipulates that citizens and organisations must provide the necessary support and assistance to public security organs, state security organs, or related organs to protect national security[91]. Article 7 of the National Security Law states that preservation of national security shall follow the Chinese Constitution and respect and protect citizens' rights under the law. However, it is unclear how the right to privacy or data protection may be invoked against these security organisations.

v. The National Intelligence Law

National Intelligence Law imposes obligations on organisations and citizens to support and cooperate with Chinese national intelligence agencies[92]. This law is described as codification of expectations that

[88] Cybersecurity Law of the PRC 2017, viewed 28 July 2021, https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-cybersecurity-law-peoples-republic-china/.
[89] Wang, Z., 2017, 'Systematic Government Access to Private-Sector Data in China' in Fred C. and Dempsey, J. (ed), '*Bulk Collection: Systematic Government Access to Private-Sector Data*, Oxford University Press, pp. 241-258, p. 245, viewed 28 July 2021, https://oxford.universitypressscholarship.com/view/10.1093/oso/9780190685515.001.0001/oso-9780190685515-chapter-11.
[90] Ji, H. and Fang, J., 2017, 'Costs and unanswered questions of China's new cybersecurity regime', viewed 28 July 2021, https://iapp.org/news/a/costs-and-unanswered-questions-of-chinas-new-cybersecurity-regime/.
[91] National Security Law of the PRC 2015, viewed 28 July 2021 https://www.chinalawtranslate.com/en/2015nsl/#_Toc423592313.
[92] National Intelligence Law of the P.R.C. 2017, viewed 28 July 2021, https://www.chinalawtranslate.com/national-intelligence-law-of-the-p-r-c-2017/?lang=en.

every citizen is responsible for state security[93]. More precisely, Article 14 of the National Intelligence Law states that the national intelligence work institutions may request companies or citizens to provide the necessary support[94]. This rule also applies to Chinese entities and their subsidiaries in foreign countries[95]. Considering the vague scope of the powers given to Chinese intelligence agencies[96], companies can be requested to access personal data. These requests cannot be denied[97]. Recent research[98], covering a security and privacy analysis of TikTok and Douyin, developed by ByteDance, found that it remains unclear whether China requested personal data access for intelligence purposes from both companies[99]. Similar concerns are raised for Huawei and its relationship with China's intelligence authorities[100]. On the other hand, according to Huawei, China's national intelligence law or other laws do not compel Huawei to install so-called "backdoors" in telecommunications' infrastructure to help government authorities to spy on other countries[101].

vi. The Counter-espionage Law

The Counter-espionage Law of the PRC[102] is another legal act that must be taken into consideration. Article 3 considers state security organs as competent authorities in charge of counter-espionage efforts. According to Article 38 of this law, espionage conducts are activities endangering state security in general. However, Article 38(3) of this law refers to "other espionage activities" while defining the scope of espionage activities, which makes it ambiguous and vague. Thus counter-espionage efforts *as such* are not explicitly defined. While conducting counter-espionage, state security organs can use technical investigative measures subject to strict formalities[103].

In addition, Article 4(1) of this law stipulates that citizens have a duty to protect national security, honour and interests and shall not jeopardise them. In light of this, all citizens, enterprises and organisations are obliged to stop espionage conducts[104]. Chapter III of the Counter-espionage Law further regulates the duties and rights of citizens and organisations in terms of counter-espionage. Especially striking is the fact that relevant organisations must provide information to the security organs[105]. There is a reference to the strict formalities and getting approval for the use of technical investigative measures by state security organs. Despite an explicit reference to the strict formalities in Article 12, the conditions of those formalities remain unclear. Therefore, this measure is most probably to include personal data, including of foreigners[106].

---

[93] Hoffman, S. and Attrill, N., 2021, 'Mapping China's Technology Giants: Supply chains and the global data collection ecosystem', viewed 28 July 2021, https://www.aspi.org.au/report/mapping-chinas-tech-giants-supply-chains-and-global-data-collection-ecosystem.

[94] Tanner, M. S., 2017, 'Beijing's New National Intelligence Law: From Defense to Offense', viewed 28 July 2021 https://www.lawfareblog.com/beijings-new-national-intelligence-law-defense-offense.

[95] Mannheimer Swartling, 2019, 'Applicability of Chinese National Intelligence Law to Chinese and non-Chinese Entities', viewed 28 July 2021, https://www.mannheimerswartling.se/app/uploads/2021/04/msa_nyhetsbrev_national-intelligence-law_jan-19.pdf.

[96] *Ibid.*

[97] *Ibid.*

[98] Lin, P., 2021, 'Tiktok v. Douyin A Security and Privacy Analysis, viewed 28 July 2021, https://citizenlab.ca/2021/03/tiktok-vs-douyin-security-privacy-analysis/.

[99] *Ibid*

[100] Kenyon, M., 'Christopher Parsons Delivers Testimony to Special Committee on Canada-China Relations' viewed 28 July 2021 https://citizenlab.ca/2021/03/christopher-parsons-delivers-testimony-to-special-committee-on-canada-china-relations/.

[101] Huawei, 2021, Huawei Facts, https://www.huawei.com/uk/facts/question-answer/hw-cooperate-with-chinas-intelligence-community-how-can-we-trust-you.

[102] The Counter-espionage Law of the PRC 2014, viewed 28 July 2021, https://www.chinalawtranslate.com/en/anti-espionage/.

[103] Art. 12 Counter-espionage Law.

[104] Art. 4(2) Counter-espionage Law.

[105] Art. 22 Counter-espionage Law.

[106] Australian perspective on Huawei and the ambiguity of China's intelligence and counter-espionage law, see Hoffman S. and Kania, E., 2018, 'Huawei and the ambiguity of China's intelligence and counter-espionage laws', viewed 28 July 2021, https://www.aspistrategist.org.au/huawei-and-the-ambiguity-of-chinas-intelligence-and-counter-espionage-laws/.

2.1.2.2 Conditions

In summary, law enforcement and intelligence agencies have widespread powers to access all forms of information where appropriate for criminal investigations or intelligence operations. New legislation at national level necessitates the development of more detailed implementing rules or policies by other State-level authorities[107]. This is a common strategy in Chinese legislation and law enactment/implementation[108]. The scope of meaning of terms such as national security, state security, or criminal investigations are broad. In addition, investigations and operations do not need to be specific nor narrowly defined.

Information access may involve access to personal data transferred to China for commercial purposes. Although the PRC's legislation governing data access includes references to "in accordance with law" or "strict approval", it is unclear which law is being referred to in these laws. Moreover, no explicit safeguards are included in these laws. In the specific legislation mentioned, the focus of those provisions is to provide support and information to the government authorities, without stipulating any specific safeguards or conditions applicable to government access.

However, the Cybersecurity Law imposes obligations on network operators in respect of their handling of personal data. Those obligations might have an indirect impact on personal data access by government authorities. For instance, network operators must comply with legality, legitimacy and necessity when collecting and using personal information (Article 41 of the Cybersecurity Law). The same article states that network operators shall avoid collecting personal information that is unrelated to the services offered. As these obligations are imposed on network operators, these provisions may represent safeguards for the initial handling of personal information by network operators. In other words, during their handling, network operators are obliged to process information proportionate to their activities. This may result in lower volumes of data processed, with a subsequent impact on the scope of information the government can access. It must be borne in mind that the law provides no specific safeguards for government access to that information. This highlights a fundamental truth of data governance in the Chinese market: while the Chinese government works to safeguard users from cyber criminals, individuals and enterprises cannot expect their data to be secure from the State[109].

2.1.2.3 Oversight

When it comes to Chinese data protection law, it should be mentioned that Article 26 of the National Intelligence Law refers to the fact that national intelligence institutions shall supervise and oversee the staff's compliance with laws and discipline. As understood from this provision and the general framework of the law, the oversight mechanism is internally established. With regard to the oversight of counter-espionage activities, Article 12 of the Counter-espionage law provides for the "strict formalities" and approval mechanisms for the use of technical measures. However, the conditions and the procedure that apply, are not clear. In other words, there is no independent supervision structure in place to review data processing activities and to whom data subjects can file complaints if they believe their data protection rights have been violated in those laws.

2.1.3 Data subject rights and redress mechanisms

2.1.3.1 Conditions

i. General

[107] According to the interview with an expert.
[108] *Ibid.*
[109] Laskai L. and Segal A., 2021, 'The Encryption Debate in China: 2021 Update', viewed 14 October 2021, https://carnegieendowment.org/2021/03/31/encryption-debate-in-china-2021-update-pub-84218

In general, the Chinese legal system does not provide data subjects with effective remedies in case of violation of their rights due to access to personal data by law enforcement or intelligence agencies. However, according to the State Council Open Government Information Regulations, individuals can seek to access and request correction of personal information in the government files and litigate the administrative organ's response[110]. To what extent this law applies to the files held by public security and national security organisations is not clear. This presents a problem as numerous state authorities applying the aforementioned laws can be military authorities, which are exempt from the administrative review. After all, no specialised courts and procedures for military authorities' oversight are present in the PRC. This is even more problematic in light of the doctrine of civil-military fusion, broadly applied in China. This entails the fact that there is close cooperation between civil and military institutions, blurring their roles in relation to national security.

According to information gathered through an interview, it can be considered that the Chinese government is not easily held accountable[111]. In order to claim rights against the government there is a need for public law basis, but this is often non-existent. Moreover, there were cases where the citizens claimed their right to information and the government claimed the right to privacy, as a safeguard against the access of citizens to information about the government. Thus, the right to privacy was claimed instrumentally by the government and was accidental to the main issue of the case.

ii. Criminal investigations

There are no provisions in place to protect the rights of suspects[112]. This is due to the fact that the collection of evidence during a criminal investigation is considered an investigative practice under the Chinese Criminal Procedural Law. This entails that police officers can choose to collect evidence without the approval of prosecutors or judges[113]. This gives these authorities leeway to investigate, resulting in violations of privacy rights[114].

Some scholars state that the violation of the right to privacy and the right to data protection during the investigation stage is not stipulated as a basis for a remedy against the authorities under Article 12 of the Administrative Procedure Law[115]. According to Articles 15 and 16 of the State Compensation Law[116], compensation may be awarded in cases of violation of the right to liberty or property right during the investigation procedure. However, there is no legal basis for compensation for the alleged violation of the right to privacy during the criminal investigation process. Consequently, it can be argued that remedies against state authorities when infringing the right to privacy are restricted.

Given the expansive nature of the authority granted to security organs or police officers, accessing the personal data of foreign individuals does not seem to be unlawful. According to Article 33 of the State Compensation Law, foreigners in the territory of China can enjoy the same rights. As a result, even if compensation rights were available, foreigners residing outside China might not benefit from compensation under the State Compensation Law, on the basis that there is a reference to foreigners residing on the territory of China. On top of that, it is necessary to appoint a PRC-based lawyer to claim

[110] Horsley, J. P., 2021, 'How will China's privacy law apply to the Chinese state?', viewed 28 July 2021, https://www.newamerica.org/cybersecurity-initiative/digichina/blog/how-will-chinas-privacy-law-apply-to-the-chinese-state/.
[111] According to the internal interview with an expert.
[112] Yang, F. and Feng, J., 2021, 'Rules of electronic data in criminal cases in China', International Journal of Law, Crime and Justice, Vol. 64, pp. 1-11, https://www.sciencedirect.com/science/article/pii/S1756061620304882#:~:text=The%20amendment%20to%20the%20Criminal,physical%20evidence%20nor%20documentary%20evidence. p. 11.
[113] *Ibid*, p. 9.
[114] *Ibid*, p. 11.
[115] *Ibid*, p. 10. When the law itself is checked, Article 11 of the Administrative Procedure Law of the People's Republic of China stipulates possible basis for administrative law cases, see Administrative Procedure Law of the PRC, viewed 19 August 2021, http://www.npc.gov.cn/zgrdw/englishnpc/Law/2007-12/12/content_1383912.htm.
[116] State Compensation Law of the PRC, viewed 19 August 2021, http://www.china.org.cn/china/LegislationsForm2001-2010/2011-02/12/content_21905705.htm.

rights in a Chinese court. This can be an additional hurdle.

iii. The Cybersecurity Law

When it comes to the data subject rights under Cybersecurity Law[117], Article 43 grants people the right to request to delete or correct their personal information if it violates provisions of the law, legislation, or agreements between data subjects and network service providers. Since these responsibilities are aimed at network providers, these rights can only be invoked against them. There are no specific protections against state authorities under this law.

iv. The National Security Law

Although the National Security Law[118] recognises human rights, it does not specify how these rights are protected. According to Article 82 of this law, citizens and organisations have the right to initiate complaints regarding 'national security efforts' if these activities are unlawful. Article 83 stipulates that extraordinary measures restricting the freedom and rights of citizens, shall be bound by actual needs and have to be in accordance with the law. However, the real question is how far the processing of personal data might be considered unlawful if personal data is accessed or processed for the tasks provided to national security organs in national security law. In other words, even though there is a right to initiate complaints regarding national security efforts, the broad construction of national security efforts might have as a result that the personal data access by state organs is not unlawful. Thus, this complaint mechanism might not work. Also, the scope of human rights is not provided under this law. Given the fact that there are no clear data subject rights for PRC civilians, it remains unclear to what extent data subjects in foreign countries can exercise complaint rights.

v. The National Intelligence Law

Article 19 of the National Intelligence Law[119] holds that the support and cooperation of civilians needs to be in accordance with the law and cannot violate lawful rights and interests of citizens and organisations. It is also held that personal information must not be leaked. However, how these rights are safeguarded against possible abuses, is unclear. Also, the law does not mention remedies for foreign citizens in case their data would be the subject of an investigation[120].

In addition, Article 27 of this law states that national intelligence agencies must have certain channels for input or complaints. However, how these complaints are treated and the nature of these complaint mechanisms are not defined. Potentially complaints can be made directly to internal organs within intelligence agencies, such as the 'discipline and inspection bureau', which is responsible for discovering and punishing internal unlawful, unprofessional conduct. This bureau is part of the CCP's internal sections formed within state authorities. Furthermore, Article 31 of the National Intelligence Law notes that national intelligence working institutions violating citizens' lawful rights or interests, will be punished in accordance with the law. However, given the fact that these mechanisms are aimed for abuse of powers in the context of intelligence activities, they might not be appropriate for data government access. This is due to the fact that access by government authorities might not be unlawful according to Chinese law.

[117] Cybersecurity Law of the PRC 2017, viewed 28 July 2021, https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-cybersecurity-law-peoples-republic-china/.
[118] National Security Law of the PRC 2015, viewed 28 July 2021, https://www.chinalawtranslate.com/en/2015nsl/#_Toc423592313.
[119] National Intelligence Law of the P.R.C. 2017, viewed 28 July 2021, https://www.chinalawtranslate.com/national-intelligence-law-of-the-p-r-c-2017/?lang=en.
[120] According to the interview with an expert.

2.1.4 Are the new laws on data protection in the PRC a game-changer for government access?

The long-awaited PRC's Personal Information Protection Law (Draft) (PIPL), the country's first comprehensive personal data protection legislation, was released in October 2020. China announced the second draft of the PIPL in April 2021. Afterwards, another round of consultations followed, then lawmakers unveiled the final draft version of the law[121]. The PIPL was adopted on 20 August 2021 and is effective as of 1 November 2021[122].

Article 1 of the PIPL provides that the law aims to protect personal information and safeguard the free flow of personal information, stimulating reasonable use of data[123]. However, it has undertones of 'national security'[124]. For instance, according to Article 10, no organisation or individual may engage in personal information handling that harms national security or the public interest. This can be seen in Chapter III, on the cross-border provision of personal information. Article 41 states that personal information handlers may not transfer personal information kept on the PRC mainland to foreign judicial or law enforcement agencies without the approval of its competent authorities. Article 42 states that where foreign organisations or individuals engage in personal information handling acts that harm the PRC's national security or public interest, the State cybersecurity and informatisation department may place them on a list limiting or prohibiting personal information provision, issue a warning, and/or implement measures such as limiting or prohibiting personal information provision.

This law will apply to both public and private organisations since no derogation is provided under Article 72. Additionally, Article 33 stipulates that PIPL applies to the activities of state organs regarding handling of personal information. However, specific provisions in Section III PIPL apply. After briefly explaining the general provisions applicable to State organs and private organisations, the specific provisions will be examined.

Chapter I of the PIPL covers the general provisions. While Article 5 refers to general principles of legality and necessity, Article 6 describes purpose limitation and data minimisation principles. The openness and transparency principle (Article 7), accuracy principle (Article 8) and data security principle (Article 9) are provided as general principles of personal information handling. Article 19 states that personal information retention periods shall be the shortest period necessary to fulfil the aim of the personal information handling, unless laws or administrative regulations stipulate otherwise. This provision is related to the data retention responsibility of personal information handlers. However, there is a reference to the laws and administrative rules that provide exceptions for these rules.

When it comes to the provisions specifically applicable to State organs in Section III, Article 34 states that they may handle personal information in accordance with the powers and procedures provided in laws or administrative regulations. Handling of personal data may not extend the scope necessary to carry out their responsibilities. Even though the Law applies to State organs, it has vague and undefined exceptions under Articles 35, which provides exceptions for the notification obligations where a provision in law or administrative regulation allows for such exception. This provision applies to all State organs regardless of their function. Article 36 states that personal information handling by State organs shall be stored within the mainland territory of the PRC. Considering the broad powers given to the State organs in national intelligence law, criminal procedural law and counter-intelligence law, those

[121] Koty, A. C., 2021, 'Personal Data Regulation in China: Personal Information Protection Law, Other Rules Amended' viewed 28 July 2021, https://www.china-briefing.com/news/personal-data-regulation-in-china-personal-information-protection-law-other-rules-amended/.
[122] https://npcobserver.com/legislation/personal-information-protection-law/, viewed 20 August 2021.
[123] https://digichina.stanford.edu/news/translation-personal-information-protection-law-peoples-republic-china-effective-nov-1-2021, viewed 23 August 2021.
[124] Dorwart H. and others, 2021, 'China's New Comprehensive Data Protection Law: Context, Stated Objectives, Key Provisions, viewed 23 August 2021, https://fpf.org/blog/chinas-new-comprehensive-data-protection-law-context-stated-objectives-key-provisions/.

provisions are less likely to limit the discretion of State authorities, as they can provide exceptions within administrative regulations. Whether this law will be enforceable in practice against State organs has been questioned[125].

Chapter IV of the PIPL covers individual's rights in personal information handling activities. As a rule, these rights can be taken to also apply to State organs, for a number of reasons. Firstly, Article 3 of the PIPL stipulates that it applies to operations involving the handling of natural persons' personal information within the PRC boundaries. Secondly, while Article 33 specifically states that PIPL applies to State organs and specific provisions of Section III apply to State organs, Chapter IV, on individual rights, states that those rights can be invoked against State organs since there is no absolute exemption for State organs.

Chapter IV of the PIPL provides individual rights, similar to data subject rights, such as "the right to know" and "the right to decide relating personal information and to limit or refuse the handling of personal information" (Article 44). Those rights can be restricted by law and administrative regulations (Article 44). There are other data subject rights: the right to access (Article 45), the right to correction (Article 46), or the right to deletion of incorrect or illegally obtained information, as well as various protections and remedies for infringements by personal information handlers (Article 47).

There are some vague exceptions for the personal information handling activities of State organs under Articles 44-45. Article 44 states that rights provided under this article exist only as long as laws or administrative regulations stipulate otherwise. This means that those rights can be restricted by other laws or regulations, providing leeway for the government authorities to fulfil those obligations. Article 45, on the right of access, refers to Article 18(1) and Article 35 of the PIPL. Article 18 provides exceptions for the transparency obligations of personal information handlers and refers to laws or administrative regulations that provide confidentiality. Therefore, as long there is a confidentiality requirement under domestic law or administrative regulations, those rights cannot be invoked. Article 35 states that if the notification duty of State organs impedes their fulfilment of their statutory duties, they will not notify individuals about personal information processing. Considering the broad powers given to State organs in the laws outlined above, it is less likely that those rights will be invoked against the State organs responsible for public security and national security.

Article 68 PIPL establishes complaint procedures, and Article 65 states that every individual has the right to file a complaint in the event of improper handling of personal information. According to Article 68 PIPL, if personal information handlers breach personal information rights and interests, individuals can claim compensation from a PRC's Court if this infringement causes any harm. This clause seems to extend to both government and private organisations.

Concerning the oversight mechanisms, Chapter VI of the PIPL specifies state departments' responsibilities to oversee the personal information handling activities. While the State Cybersecurity and Informatisation department is charged with comprehensive planning and management, relevant State Council's departments are accountable for the protection and overseeing of personal information. It seems that these departments are structured in the general government structure and designed accordingly. Although these departments are equipped with proper tools for the investigation and enforcement[126], there are no standards set for these supervisory mechanisms' independence. If state authorities indulge in improper personal information handling practices, their superior organs or

[125] Greenleaf, G., 2020, 'China issues a comprehensive draft data privacy law', Privacy Laws & Business International Report Vol. 168, No. 1, pp. 6-10, viewed 28 July 2021, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3795001; Harsley provides a comprehensive analysis of applicability of data protection framework to the state organs, including the Draft PIPL, see Horsley, J. P., 2021, 'How will China's privacy law apply to the Chinese state?', viewed 28 July 2021, https://www.newamerica.org/cybersecurity-initiative/digichina/blog/how-will-chinas-privacy-law-apply-to-the-chinese-state/.

[126] Article 59 of Personal Information Protection Law of the People's Republic of China (Draft) (Second Review Draft), viewed 28 July 2021, https://digichina.stanford.edu/news/translation-personal-information-protection-law-peoples-republic-china-draft-second-review.

agencies charged with personal information security must order correction according to Article 68 of the PIPL. This clause confirms that the PIPL only establishes an internal oversight mechanism. Even if these developments can be viewed as improving individuals' positions against Chinese state authorities, they do not meet the EU-Charter nor the CJEU case-law expectations.

In addition, the Data Security Law (DSL) was passed following three rounds of deliberations on 10 June 2021, this at the 29th session of the 13th NPC. As of 1 September 2021, the DSL[127] takes effect in China[128]. The DSL aims at ensuring data security, promoting data development, protecting the lawful rights and interests of individuals and organisations and safeguarding national sovereignty, security and development interests[129]. According to Article 2 of the DSL, the law applies to data handling activities and their security regulation. Article 2(2) of the DSL provides for the extraterritorial application of the DSL as long as data handling activities outside of the mainland territory of the PRC harm national security, public interest, and other interests mentioned in the Article. The DSL will bring differentiated security obligations depending on the classification of data as "important data" and "core national data" according to Article 21 of the DSL[130]. With respect to the reference to the protection of personal data, Article 53 of the DSL states that data handling operations involving personal information must also adhere to the provisions of applicable laws and administrative regulations. This provision leaves room for the application of the PIPL. It is argued that the DSL, as well as the PIPL, are applicable to the security of personal data. After all, the DSL is applicable to the data handling activities regardless of the classification of personal data and non-personal data[131].

2.1.5 Intermediary conclusion

The main legal instruments identified during the study, which relate to the government access to personal data of individuals, are summarised in the table below. This table briefly shows the analysis of the scope of government access, oversight mechanisms, redress mechanisms and data subject rights. According to Article 44 of the GDPR, any transfer of personal data to a third country shall take place only if it complies with Chapter 5 of the GDPR and other provisions of the GDPR. As it is discussed in Section 1.2 of this Report, the law of third countries shall provide equivalent level protection to the data subjects in the EU.

The first concern is to what extent the scope of government access to personal data is delineated to meet legality requirement in accordance with the EU-Charter. As shown in the table, the analysed legislation imposes technical support and assistance on citizens and organisations without restricting access of government to the personal data. Even though there is a reference to "in accordance with law" in a legislative framework such as cybersecurity law, the law itself does not provide for any limitation on government data access. It might be concluded that those rules would not meet the legality requirement provided under the EU-Charter. Oversight mechanism, redress mechanisms and data subject rights are crucial to meet the proportionality requirement, which is discussed in Section 1.2 of this Report. For the oversight mechanism of the government access, the laws stipulate internal mechanisms without providing any assurance of the independence of those mechanisms. When it comes to the redress mechanisms and data subject rights, as shown in the table, both of them are limited in the case of government access.

All in all, the examination of these secondary legislation reveals that the government has some leeway

[127] Data Security Law of the PRC 2021, viewed 28 July 2021, https://digichina.stanford.edu/news/translation-data-security-law-peoples-republic-china.
[128] Susan, N. and others, 2021, 'China Data Protection Paths under Data Security Law' viewed 28 July 2021, https://www.chinalawinsight.com/2021/06/articles/uncategorized/china-data-protection-paths-under-data-security-law/#_ftn3.
[129] Article 1 DSL.
[130] Susan, N. and others, 2021, 'China Data Protection Paths under Data Security Law' viewed 28 July 2021, https://www.chinalawinsight.com/2021/06/articles/uncategorized/china-data-protection-paths-under-data-security-law/#_ftn3.
[131] *Ibid.*

in acquiring people's data. It is possible to argue that Chinese legislation legitimises the government's vast and unlimited access to personal data. The PIPL and Data Security Law (DSL) could be viewed as an effort to improve data protection in the PRC. Those improvements are specific provisions on general data processing principles (legality, proportionality, data minimisation, purpose limitation), which are applicable to all State organs. Individual rights in respect of personal information are granted to individuals. However, the oversight mechanism is internally structured within the State organ, with no independence mandated by law.

Those changes do not, however, make a significant difference in relation to what the PRC government will be allowed to do with people's data. Firstly, exceptions can be foreseen in law and administrative regulation, allowing government authorities to circumvent the restrictions provided under the PIPL. Secondly, any substantial change and broadening of the scope of protection would require changes to the Constitution and, in effect, changes to the political system. The provisions of secondary law with regard to access to personal data by the government are immaterial as long as the Constitution and political system legitimise unrestrained access to personal data.

Laws/ Features	Scope of Government Access	Oversight	Redress Mechanism/Data Subjects' Rights
Laws related to the criminal investigations	Electronic data including personal data stored in domestic computer systems. Only publicly available electronic data stored abroad.	Internal oversight	No right to sue in the violation of privacy rights in the phase of investigation in both Administration Litigation Law and State Compensation Law.
National Security Law	The necessary support and assistance obligation on citizens and organisations.	Internal oversight	Initiating complaints regarding "national security efforts" if these activities are unlawful.
National Intelligence Law	The necessary support and assistance obligation on citizens and organisations.	Internal oversight	National intelligence agencies must have certain outlets for input or complaints about their activities.
Counter-espionage Law	Using technical investigative measures for investigation activities. The necessary support and assistance obligation on citizens and organisations.	Internal oversight (reference to strict formalities without clarifying the scope of formalities)	Unclear
Cybersecurity Law	Network operators must provide "technical support and assistance" in accordance with the law, including content and metadata[132].	N/A	It grants individuals the right to request that their personal information be deleted or corrected against network providers.
PIPL (effective as of 1 November 2021)	No specific provision on government access. However, general principles of information handling (legality, transparency, purpose limitation, data minimisation, principle of data security	Internal oversight for State organs	It grants individuals rights, such as the right of access and right of correction, with possible exceptions

[132]Ji, H. and Fang, J., 2017, 'Costs and unanswered questions of China's new cybersecurity regime', viewed 28 July 2021, https://iapp.org/news/a/costs-and-unanswered-questions-of-chinas-new-cybersecurity-regime/.

	and storage limitation) are applicable to the State organs, with possibility of exceptions under other laws or administrative regulations.		under other laws and administrative regulations.

2.2 INDIA

2.2.1 Rule of law, respect for human rights and fundamental freedoms

2.2.1.1 Context

India is a multiparty, federal, parliamentary democracy with a bicameral legislature[133]. It is founded on a common law system, owing its origins to the colonial period of England[134]. Under the Constitution, the country's 28 states and eight union territories have a high degree of autonomy and have primary responsibility for law and order[135].

The Constitution of India stipulates that the country is governed by the rule of law, meaning that any legislation failing to comply with the Constitution and its fundamental rights will be declared invalid (Article 13(1)). Several fundamental rights are laid down in the Constitution, such as freedom of speech (Article 19), and protection of life and personal liberty (Article 21)[136]. In terms of fundamental human rights, it is worth noting that India has a national human rights' commission, which was established in 1993[137]. In addition to its national legislation, there are several international human rights' treaties to which India is bound. Relevant for this study are in particular the Universal Declaration of Human Rights (UDHR)[138] and the International Covenant on Civil and Political Rights (ICCPR)[139]. Both treaties acknowledge the right to privacy (Article 12 UDHR and Article 17 ICCPR)[140].

The right to privacy and the right to data protection have taken a controversial path in India. Although the Constitution does not recognise the right to privacy, the 2017 *Puttaswamy v. Union of India* decision of the Supreme Court of India explicitly acknowledged it as a fundamental right[141]. In this landmark judgment, the Court ruled that the right to privacy is implied in Article 21 of the Constitution and is incidental to other freedoms guaranteed by the Constitution[142]. In fact, the Court stated that the constitutional right to privacy can only be enforced against (bodies of) the State and not against civilians or private sector entities[143]. However, the Court held that the right to privacy is enforceable against non-State entities on the basis of other national legislation, thus a robust regime for data protection should

[133] National Portal India, viewed 27 May 2021, https://www.india.gov.in/my-government.
[134] Baxi, U., "The Colonialist Heritage" in Pierre Legrand and Roderick Munday (eds.), Comparative Legal Studies: Traditions and Transitions, Cambridge University Press, 2003, pp. 6-58.
[135] National Portal India, viewed 27 July 2021, https://www.india.gov.in/my-government.
[136] Constitution of India, viewed 12 July 2021, https://legislative.gov.in/sites/default/files/COI_1.pdf.
[137] This committee was established under the national act on the protection of human rights (adopted in 1993) and amended in 1997, 2006 and in 2019; National human rights commission, India, viewed 27 May 2021, https://nhrc.nic.in/.
[138] National human rights commission, India, viewed 27 May 2021, https://nhrc.nic.in/acts-&-rules/declarationcovenants-1.
[139] India accessed this treaty in 1979; see Ratification of International Human Rights Treaties-India, viewed 27 May 2021, http://hrlibrary.umn.edu/research/ratification-india.html.
[140] In light of the ICCPR, it is also important to refer to its general comments, which further elaborate on the meaning of the rights in the treaty. Especially general comment 16 is important as it underlines the fact that the right to privacy can be limited as long as the limitation is not arbitrary nor unlawful; ICCPR General Comment No. 16: Article 17 (Right to Privacy) The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation.
[141] Indian Supreme Court, Puttaswamy v. Union of India, 26 September 2018; Chhugani, S. (2021). India's Aadhaar card a violation of Indian citizen's right to privacy. Cardozo International & Comparative Law Review, 4(2), 733-762; X., 1.3 Billion People's Right To Privacy Upheld Following Historic Judgement By India's Supreme Court', viewed 21 June 2021, https://privacyinternational.org/blog/768/13-billion-peoples-right-privacy-upheld-following-historic-judgement-indias-supreme-court.
[142] *Ibid.*
[143] Indian Supreme Court, Puttaswamy v. Union of India, 2017, §20, https://indiankanoon.org/doc/91938676/.

be introduced[144]. In addition, the Court specifically extended this right to non-citizens, meaning that EU data subjects can potentially raise judicial claims against any infringement of Indian authorities if their right to privacy would be violated[145]. In a follow-up judgment[146], the Court held that the right to privacy can only be limited by specific legislation, providing procedural guarantees against abuse[147]. In stating so, the Court mirrored Article 52 EU-Charter and held that such legislation can only be installed for 'legitimate aims of the State' and must be 'necessary and proportionate in a democratic society'[148]. According to the opinion of local experts, the *Puttaswamy* judgment has changed the attitude towards the right to privacy in India. After all, the decision recognised multiple facets of the right to privacy, such as informational privacy, sexual privacy and bodily privacy. Due to the large material scope of the judgment, other rights connected to the right to privacy were also subsequently recognised by Indian courts, such as the right to be forgotten[149].

In the aftermath of this jurisprudence, an Indian Group of Experts on Privacy, appointed by the government, reported that India lacked a comprehensive data-protection framework[150]. As a result of the findings of this group, the Indian government released a draft legislation on Personal Data Protection (PDP Bill) for consultation in 2019[151]. The PDP Bill seeks to regulate the processing of personal information by Indian entities and, in certain specific circumstances, offshore entities[152]. However, this Bill has not yet been adopted (see section 2.2.4: Upcoming changes in legislation).

Currently, data privacy in India is primarily addressed in the Information Technology Act (IT Act)[153]. However, the State falls outside the scope of the safeguards for privacy in the processing of personal data[154]. In addition, various sector-specific regulations regarding data governance were adopted in India[155]. In light of this, the Reserve Bank of India, India's central banking authority, issued directions for all banks and their service providers, intermediaries, third party vendors and other entities in the payment ecosystem[156]. By virtue of this regulation, all payment system data, including the entire

---

144 Indian Supreme Court, Puttaswamy v. Union of India, 2017, p. 264, https://scobserver-production.s3.amazonaws.com/uploads/case_document/document_upload/628/1-266Right_to_Privacy__Puttaswamy_Judgment-Chandrachud.pdf.

145 Indian Supreme Court, Puttaswamy v. Union of India, 2017, §20, https://indiankanoon.org/doc/91938676/.

146 The Aadhaar Card (and other measures of the Indian government) also has effect on other rights such as the right against discrimination. After all, there are several people who struggle to provide their biometrics, such as elderly and disabled persons. Also, this right is enshrined in the Indian Constitution, which ensures that all citizens are equal and that no person shall be discriminated on the basis of sex, religion, race or place of birth (Article 15 Constitution). In addition, India has international obligations in this area as it ratified international treaties such as the International Convention on the Elimination of All Forms of Racial Discrimination and the Convention on the Elimination of All Forms of Discrimination against Women. Until now, the Supreme Court has not spoken out on this matter.

147 Indian Supreme Court, Puttaswamy v. Union of India, 26 September 2018, §377, https://indiankanoon.org/doc/91938676/.

148 *Ibid.*

149 According to an internal interview with a local expert.

150 Save our Privacy, 27 July 2018, Initial statement on justice Srikrishna committee report, viewed 27 May 2021, https://saveourprivacy.in/blog/initial-statement-on-justice-srikrishna-committee-report.

151 *Ibid.*

152 Article 2(A) Personal Data Protection Bill: *The provisions of this Act shall apply to (a) the processing of personal data where such data has been collected, disclosed, shared or otherwise processed within the territory of India; (b) the processing of personal data by the State, any Indian company, any citizen of India or any person or body of persons incorporated or created under Indian law; (c) the processing of personal data by data fiduciaries or data processors not present within the territory of India, if such processing is (i) in connection with any business carried on in India, or any systematic activity of offering goods or services to data principals within the territory of India; or (ii) in connection with any activity which involves profiling of data principals within the territory of India.* Viewed 27 May 2021, https://prsindia.org/files/bills_acts/bills_parliament/Personal%20Data%20Protection%20Bill,%202019.pdf.

153 Chowdhury, P., Thayil, K., 25 January 2021, Data Privacy in India, viewed 27 May 2021, https://www.mondaq.com/india/privacy/1005640/data-privacy-comparative-guide?.

154 Deva Prasad, M., and Suchita Menon, C., 2020, The Personal Data Protection Bill, 2018: India's regulatory journey towards a comprehensive data protection law, *International Journal of Law and Information Technology*, 2020, pp. 1-19.

155 Chowdhury, P., Thayil, K. 25 January 2021, Data Privacy in India, viewed 27 May 2021, https://www.mondaq.com/india/privacy/1005640/data-privacy-comparative-guide.

156 X., 18 June 2020, India: RBI publishes framework on payment system operators, viewed 25 May 2021, https://www.dataguidance.com/news/india-rbi-publishes-framework-payment-system-operators.

payment processing cycle from request to final pay-out, need to be stored on the territory of India[157]. Furthermore, the Insurance Regulatory and Development Authority of India, the principal regulator of the Indian insurance industry, published regulations that govern all outsourcing arrangements entered by Indian insurers[158]. Lastly, the Securities and Exchange Board of India, the regulator for the securities market, has issued regulations prescribing mandatory security breach notification requirements that cover instances of data theft or breach[159].

2.2.1.2 General findings of international organisations

Several international organisations have looked into the human rights situation in India. In general, conditions in India can be improved in several areas such as freedom of expression and the fight against discrimination[160]. Also, the state-of-the-art with respect to privacy and data protection can be enhanced. Various organisations have highlighted the lack of application of privacy related legislation to State conduct[161]. A recent example can demonstrate this further. In 2017, India had to conduct a Universal Periodic Review (UPR)[162]. Observant states were concerned that the PDP Bill would be hollowed out as Indian agencies enjoyed many exemptions from this bill[163]. It was stressed that the bill did not meet international standards[164].

2.2.2 Government access to personal data

2.2.2.1 Purposes

i. The Information Technology Act

The IT Act was adopted in 2000 and addresses the collection of personal data for surveillance purposes. Although the initial legislation provided for several standards in relation to government access to data, the IT Act amendment of 2008 substantially weakened these[165].

Currently, Section 69 of the IT Act dictates that the government may access any possible computer source and collect every piece of information stored on it, if this is in the interest of national security and the prevention of crimes[166]. To this end, the government may issue directions to any governmental agency to intercept, monitor or decrypt such information[167]. Furthermore, Section 69B of the IT Act allows the government to authorise any agency to monitor and collect any traffic data and information

[157] Chowdhury, P., Thayil, K., 25 January 2021, Data Privacy in India, viewed 27 May 2021, https://www.mondaq.com/india/privacy/1005640/data-privacy-comparative-guide.
[158] *Ibid.*
[159] *Ibid.*
[160] HRW, 2020, Indian Events of 2020, viewed 3 June 2021, https://www.hrw.org/world-report/2021/country-chapters/india.
[161] Deva Prasad, M., and Suchita Menon, C., 2020, The Personal Data Protection Bill, 2018: India's regulatory journey towards a comprehensive data protection law, *International Journal of Law and Information Technology*, 2020, pp. 1-19.
[162] This is a human rights review process established by the United Nations Human Rights Council. It was already the third time, previous cycles dated from 2012 and 2008.
[163] UN General Assembly, Human Rights Council, Summary of Stakeholders' submissions on India, February 2017, https://documents-dds-ny.un.org/doc/UNDOC/GEN/G17/046/29/PDF/G1704629.pdf?OpenElement; Article 35 PDP Bill.
[164] *Ibid.*
[165] A 1997 decision established certain safeguards under India's long-standing Telegraph Act of 1885 governing telephone interception but succeeded due to the IT Act, see for more information: Rubinstein, I.S., Nojeim, G.T., Lee, R.D., 2014, Systematic government access to personal data: a comparative analysis, *International Data Privacy Law*, vol. 4(2), pp. 96–119, https://doi.org/10.1093/idpl/ipu004.
[166] Section 69 of the Information Technology Act 2000. In particular, the grounds justifying such activity of interception, monitoring or decryption are the sovereignty or integrity of India, the defence of India, the security of the State, the friendly relations with foreign countries or the public order, or the prevention of the incitement to the commission of any cognizable offense related to the same grounds. Viewed on 26 May 2021, https://www.indiacode.nic.in/bitstream/123456789/13116/1/it_act_2000_updated.pdf.
[167] *Ibid.*

in any computer sources, based on the ground of enhancing national cybersecurity[168]. Although the grounds justifying such access to personal data are enshrined in the aforementioned provisions, the IT Act does not clearly define these concepts. According to the local experts, the provisions provide a certain degree of uncertainty around the decisions of the government based on Sections 69 and 69B. The vague concepts still characterise the IT Act, notwithstanding the suggestion of the Indian judicial authorities to limit such provisions and the power of the executive therein[169].

Under these provisions, intermediaries must provide a high degree of assistance to the governmental agencies. In fact, when a request of access is issued but remains unheard, criminal liability will be imposed for the failure to provide the government with access to any information. In this case, the punishment amounts to both an imprisonment and a fine[170]. The IT Act adopts a very broad definition of "intermediary", as it includes, amongst others: telecom service providers, network service providers, internet service providers, search engines, online payment sites, online-market places[171]. In other words, any provider of digital services entitled to process personal data may be subject to the aforementioned provisions. As a result, the Indian government heavily relies on private intermediaries to conduct surveillance activities, as some of the obligations imposed to the private intermediaries are based on national security considerations which are not limited anymore to the sole public sphere[172]. Furthermore, the 2008 amendment to the IT Act extended criminal liability to any person, irrespective of his or her nationality, and regardless of where the conduct took place. The only condition which needs to be fulfilled is that such conduct involves a computer, computer system or computer network located in India[173]. Therefore, a non-Indian intermediary could also be deemed liable for denying the government access to personal data pursuant to Sections 69 and 69B.

In 2011, India installed the Centralised Monitoring System (CMS) based on Section 5(2), read together with rule 419A of the IT Act. This section empowers the Indian Government to intercept communications in a situation of "public emergency" or in the interest of "public safety". It is allowed to intercept communications in the following situations: (i) in the interests of the sovereignty and integrity of India; (ii) for the security of the State; (iii) friendly relations with foreign states; (iv) public order; (v) for preventing incitement to the commitment of an offence.

Although this section clearly mandates *targeted* surveillance, the CMS has led in practice to *mass* surveillance and bulk collection of data[174]. More precisely, the CMS requires telecom service providers to share phone and internet communications (including emails) in the country with the government[175]. Based on rule 419 A of the IT Rules 2007, these providers can retain any message or class of messages[176]. Moreover, in 2018 in light of Section 69, 10 Indian security and intelligence

[168] Section 69B of the Information Technology Act 2000: The Government may authorise any agency to monitor or collect such traffic data and information in order to enhance cybersecurity or for identification, analysis and prevention of intrusion or spread of a computer contaminant in the country. A computer contaminant is defined as "any set of computer instructions that are designed: a) to modify, destroy, record, transmit data or programme residing within a computer, computer system or computer network, or b) by aby means to usurp the normal operations of the computer, computer system, or computer network" (Section 43 of the IT Act), viewed on 29 May 2021, https://www.indiacode.nic.in/bitstream/123456789/13116/1/it_act_2000_updated.pdf.

[169] According to an internal interview with a local expert.

[170] Section 69(3) and Section 69B(4) of the Information Technology Act 2000, viewed on 29 May 2021, https://www.indiacode.nic.in/bitstream/123456789/13116/1/it_act_2000_updated.pdf.

[171] Section 2(w) of the Information Technology Act 2000, viewed on 29 May 2021, https://www.indiacode.nic.in/bitstream/123456789/13116/1/it_act_2000_updated.pdf.

[172] Bhandari, V., Sane, R., 2018, Protecting Citizens from the State Post *Puttaswamy*: Analysing the Privacy Implications of the Justice Srikrishna Committee Report and the Data Protection Bill, *Socio-Legal Review*, vol. 14(2), pp. 143-169.

[173] Section 75 of the Information Technology Act 2000.

[174] Section 5(2) IT Act;Rule 419A IT Act; Draftrule 419B IT Act; HRW, 7 June 2013, India: New Monitoring System Threatens Rights, viewed on 3 June 2021, https://www.hrw.org/news/2013/06/07/india-new-monitoring-system-threatens-rights.

[175] Section 5(2) IT Act; Art. 419A IT Act; Draft Art. 419B IT Act; HRW, 7 June 2013, India: New Monitoring System Threatens Rights, viewed on 3 June 2021, https://www.hrw.org/news/2013/06/07/india-new-monitoring-system-threatens-rights.

[176] Rule 419 A IT Act, https://cis-india.org/internet-governance/resources/rule-419-a-indian-telegraph-rules-1951; https://dot.gov.in/sites/default/files/march2007.pdf?download=1.

agencies were authorised by the Ministry of Home Affairs to carry out interception, monitoring and decryption activities[177]. It should be highlighted that this provision allows bulk interception, as the government may intercept any information, being not only data but also messages, texts, voices, images, etc.[178]. As various human rights' organisations pointed out, these powers have the potential to strongly undermine the right to data protection in India[179].

In addition, the IT Act confers to the government a broad power to adopt regulations in order to specify its provisions[180]. Therefore, the Information technology intermediary guidelines and digital media Ethics code rules (Rules 2021) were adopted in 2021[181]. The Rules 2021 are aimed at combating harmful content online, including fake news and criminal content[182]. They set obligations for social media intermediaries to implement privacy policies with specific due diligence standards and to remove certain types of content[183]. It should be noted that the rules introduce further grounds for government access to personal data. Significant social media intermediaries which primarily provide messaging services are obliged to provide the identity of the "first originator", being the first person sending a message[184]. This is required by judicial order, in the context of prevention, detection, investigation, prosecution or punishment of an offence related to national security, public order, international relations and sexually explicit material or child pornography[185]. In case the first originator is an individual located outside the territory of India, the originator of the information within the territory of India is considered to be the first originator in light of this provision[186]. Similarly to the provisions contained in the IT Act, an intermediary refusing to comply with such an order faces criminal liability[187].

ii. The Aadhaar Act

In 2015, India adopted the "Digital India" programme, aiming to transform the country into a digitally empowered society via e-governance through digital means[188]. As part of its programme, it introduced the 'Aadhaar Unique Identification Number' (Aadhaar Card), a national identification card system creating a biometric-based identity number to allow Indian citizens to access government benefits, subsidies and services[189]. To further institutionalise this project, the Aadhaar Act was adopted in 2016[190]. In order to obtain the Aadhaar card, citizens need to provide the government with a large amount of

[177] Order of the Ministry of Home Affairs (Cyber and Information Security Division) of the 20 December 2018, viewed on 14 June 2021, https://egazette.nic.in/WriteReadData/2018/194066.pdf.
[178] Section 2(W) of the Information Technology Act 2000.
[179] UN General Assembly, Human Rights Council, National report submitted in accordance with paragraph 5 of the annex to Human Rights Council resolution 16/21* India, February 2017, viewed on 30 May 2021, https://documents-dds-ny.un.org/doc/UNDOC/GEN/G17/044/56/PDF/G1704456.pdf?OpenElement.
[180] Section 87 of the Information Technology Act 2000, viewed on 1 June 2021, https://www.indiacode.nic.in/bitstream/123456789/13116/1/it_act_2000_updated.pdf.
[181] Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules 2021, viewed on 17 June 2021, https://www.meity.gov.in/writereaddata/files/Intermediary_Guidelines_and_Digital_Media_Ethics_Code_Rules-2021.pdf.
[182] International Association of Privacy Professionals (IAPP), 2021, Information Technology Rules, 2021 suggest big changes for Big Tech in India, viewed on 8 June 2021, https://iapp.org/news/a/information-technology-rules-2021-suggest-big-changes-for-big-tech-in-india/.
[183] Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules 2021, viewed on 17 June 2021, https://www.meity.gov.in/writereaddata/files/Intermediary_Guidelines_and_Digital_Media_Ethics_Code_Rules-2021.pdf.
[184] Section 4(2) of the Information Technology (intermediary Guidelines and Digital Media Ethics Code) Rules 2021, viewed on 17 June 2021, https://www.meity.gov.in/writereaddata/files/Intermediary_Guidelines_and_Digital_Media_Ethics_Code_Rules-2021.pdf.
[185] *Ibid.*
[186] *Ibid.*
[187] Section 7 of the Information Technology (intermediary Guidelines and Digital Media Ethics Code) Rules 2021, viewed on 18 June 2021, https://www.meity.gov.in/writereaddata/files/Intermediary_Guidelines_and_Digital_Media_Ethics_Code_Rules-2021.pdf.
[188] Digital India Programme, viewed on 1 June 2021, https://www.digitalindia.gov.in/.
[189] *Ibid.*
[190] Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016, viewed on 5 June 2021, https://uidai.gov.in/images/targeted_delivery_of_financial_and_other_subsidies_benefits_and_services_13072016.pdf .

personal data, including biometric and demographic data[191]. The personal data linked to the Aadhaar Card are stored in a centralised database administered by a governmental agency appointed by the government, known as the Unique Identification Authority of India (UIDAI)[192].

After the adoption of the Aadhaar Act, the Aadhaar number became the main source of identification for government bodies and private companies in a wide range of services[193]. For example, the Aadhaar number was used to certify marriages, receive welfare and pension payments, open bank accounts, access mobile phone communications and file income tax returns[194]. Furthermore, numerous provisions of the Aadhaar Card Act empower the UIDAI to adopt additional regulations about the collection of information under the scheme[195]. For example, the UIDAI has the power to adapt the list of personal data to be collected under the Aadhaar scheme[196]. Consequently, the agency has been given large discretion in setting policy matters related to the Aadhaar scheme[197].

The aforementioned *Puttaswamy* judgment also dealt with the alleged unconstitutionality of the Aadhaar Act and its mandatory nature for a large number of public and private services. Although the Supreme Court upheld its constitutionality, it overruled the mandatory nature of an Aadhaar number for non-welfare purposes and for the (entire) private sector. In the aftermath of the judgment, the Aadhaar and Other Laws (Amendment) Act was adopted in 2019[198]. However, in the view of Indian experts, the amendment only partially complies with the judgment. In fact, while the Court stated that the Government should provide citizens with alternative means to the Aadhaar scheme in order to access public welfare services, the current legislative framework still allows the Indian Parliament to make the Aadhaar authentication mandatory for specific welfare schemes[199]. Besides, the amendment of 2019 allows the Government to permit banking companies to perform authentication via the Aadhaar scheme, when necessary or expedient to do so in the context of the Indian anti-money laundering policy[200]. However, there are no provisions defining the concepts of necessity and expediency. It can be held that the excessive vagueness requiring a governmental decision on the access to personal data represents a trend across Indian legislation[201].

The provisions under the Aadhaar Act are also relevant for foreigners, as it establishes that anyone who has resided in India for at least 182 days in the 12 months preceding the application is considered a resident[202]. This means that any foreign individual applying to obtain an Aadhaar number will be included in the Aadhaar database. The Indian government will thus have access to their data in the event that a judicial order is issued by a High Court or by a high-ranking governmental officer empowered to

[191] *Ibid.*
[192] Chhugani, S., 2021, India's Aadhaar card a violation of Indian citizen's right to privacy, Cardozo International & Comparative Law Review, vol. 4(2), pp. 733-762; Privacy International, 1 December 2017.
[193] Section 7 of the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016, viewed on 5 June 2021, https://uidai.gov.in/images/targeted_delivery_of_financial_and_other_subsidies_benefits_and_services_13072016.pdf.
[194] *Ibid.*
[195] Section 2(g) of the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016, viewed on 6 June 2021, https://uidai.gov.in/images/targeted_delivery_of_financial_and_other_subsidies_benefits_and_services_13072016.pdf.
[196] *Ibid.*
[197] Bhandari, V., Sane, R., 2019, A Critique of the Aadhaar Legal Framework, *National Law School of India Review*, vol. 31(1), pp. 72-97, https://heinonline.org/HOL/Page?handle=hein.journals/nlsind31&div=9&g_sent=1&casa_token=&collection=journals.
[198] Aadhaar and Other Laws (Amendment) Act, 2019, viewed on 10 June 2021, https://uidai.gov.in/images/news/Amendment_Act_2019.pdf.
[199] According to an intern interview with an local expert.
[200] Section 27 of the Aadhaar and Other Laws (amendment) Act 2019, viewed on 5 June 2021, https://uidai.gov.in/images/targeted_delivery_of_financial_and_other_subsidies_benefits_and_services_13072016.pdf.
[201] According to an intern interview with a local expert.
[202] Section 2(v) and 3 of the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016, viewed on 5 June 2021, https://uidai.gov.in/images/targeted_delivery_of_financial_and_other_subsidies_benefits_and_services_13072016.pdf.

do so by the Government for law enforcement/national security or any other purpose[203].

2.2.2.2 Conditions

i. The Information Technology Act (Section 43A and the IT Rules 2011)

While the IT Act contains general provisions regarding the conditions for the processing of personal data, state conduct is exempt from these safeguards, leaving a legislative vacuum with regard to government access to personal data[204]. In view of this, Section 43A of the IT Act should be discussed. This Article confers the power to the government to adopt regulations to implement the IT Act[205]. In light of this delegated power, the Reasonable security practices and procedures and sensitive personal data or information rules (Rules 2011) were adopted[206]. Both Section 43A and the Rules 2011 only apply to "body corporates", being companies, firms and other associations of persons engaged in commercial or professional activities[207]. According to the Rules 2011, sensitive personal data[208] can only be collected and processed for a lawful purpose connected with a function or activity of the data collector in question, and if the collection is considered necessary for that purpose[209]. Normally, "body corporates" are obliged to obtain consent from the provider of the information before disclosing personal information. However, consent is not required when governmental agencies make a written request to access data for the purpose of verification of identity, or for the prevention, detection or investigation of crimes[210]. Such a provision is in line with the general exceptions provided under the IT Act, and enlarges the government powers, rather than limiting them. Furthermore, due to an explicit reference in the Aadhaar Act to the IT Act, biometric data collected under the Aadhaar scheme are also subject to Section 43A of the IT Act and the Rules 2011[211].

i. The Information Technology Act (Section 69 and the IT Rules 2009)

Section 69 of the IT Act gives the Indian government the power to adopt regulations establishing procedures and safeguards to be respected in the interception, monitoring or decryption of information activities. Based on this provision, the Information technology procedure and safeguards for

[203] Rule 33 Aadhaar Act.
[204] Deva Prasad, M., and Suchita Menon, C., 2020, "The Personal Data Protection Bill, 2018: India's regulatory journey towards a comprehensive data protection law", International Journal of Law and Information Technology, vol. 28, pp. 1-19, viewed on 10 July 2021, https://academic.oup.com/ijlit/article/28/1/1/5743451.
[205] Sensitive personal data or information are defined, under Section 43A of the IT Act, as "such personal information as may be prescribed by the Central Government in consultation with such professional bodies or associations as it may deem fit", viewed on 5 June 2021, https://uidai.gov.in/images/targeted_delivery_of_financial_and_other_subsidies_benefits_and_services_13072016.pdf.
[206] Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011, viewed on 6 June 2021, [भाग II- खण्ड 3(i)] भारत का राजपत्र : असाधारण 7 (meity.gov.in).
[207] Chowdhury, P., Thayil, K., 25 January 2021, Data Privacy in India, viewed on 18 June 2021, https://www.mondaq.com/india/privacy/1005640/data-privacy-comparative-guide.
[208] According to Section 3 of the IT Rules 2011, sensitive personal data or information are defined as "*such personal information which consists of information relating to: i) password; ii) financial information such as Bank account or credit card or debit card or other payment instrument details; iii) physical, physiological and mental health condition; iv) sexual orientation; v) medical records and history; vi) biometric information; vii) any detail relating to the above clauses as provided to body corporate for providing service; and viii) any of the information received under above clauses by body corporate for processing, stored or processed under lawful contract or otherwise.*" viewed on 6 June 2021, [भाग II- खण्ड 3(i)] भारत का राजपत्र : असाधारण 7 (meity.gov.in).
[209] Chowdhury, P., Thayil, K., 25 January 2021, Data Privacy in India, viewed on 18 June 2021, https://www.mondaq.com/india/privacy/1005640/data-privacy-comparative-guide.
[210] Section 6 of the Information Technology (Reasonable Security Practices and Procedures and Sensitive personal Data or information) Rules, 2011, viewed on 6 June 2021, [भाग II- खण्ड 3(i)] भारत का राजपत्र : असाधारण 7 (meity.gov.in).
[211] Section 30 of the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016, viewed on 6 June 2021, https://uidai.gov.in/images/targeted_delivery_of_financial_and_other_subsidies_benefits_and_services_13072016.pdf.

interception, monitoring and decryption of information rules (Rules 2009) were adopted[212]. According to the Rules 2009, the competence to issue an order under Section 69 lies with the Secretary in the Ministry of Home Affairs (in case of the Central Government) and with the Secretary in charge of the Home Department (in case of a local government)[213]. However, in case of unavoidable circumstances or emergencies, the order may be issued by senior officers of security or law enforcement agencies. In such cases, an *ex-ante* or *ex post* authorisation is due by the competent authority[214]. The order of the government and the reasons behind it are required to be in written format[215]. Besides, the Rules 2009 set a last resort principle, as Section 69 should only be used if no alternative means are available[216]. Such a direction should not exceed 60 days from its issue. However, the government may renew the order for a total period of 180 days[217]. The Rules 2009 also establish that the records pertaining to the interception, monitoring or decryption activities should be destroyed every six months from the governmental agency having access to the information, while the intermediaries have a period of two months to destroy such information[218]. However, the IT Act imposes an obligation on the intermediaries to preserve and retain the information for a period as prescribed by the central government[219].

Finally, while a general prohibition of disclosure of the intercepted information is established under the Rules 2009, the governmental agencies are allowed to share this information with other security agencies for the purpose of investigation of crimes or in judicial proceedings[220]. As regards the intermediaries, the principles of secrecy and confidentiality are normally applicable although these principles are exempted when the recipient is a security agency[221].

iii. The Aadhaar Act

Chapter VI of the Aadhaar Act is explicitly dedicated to the protection of information of individuals, containing general principles and conditions for handling personal data. A general obligation of security and confidentiality lies with the UIDAI, this organisation is prohibited to reveal any information collected under the Act during its service or thereafter[222]. In addition, a principle of purpose limitation

[212] Information Technology (Procedures and Safeguards for Interception, Monitoring and Decryption of Information) Rules 2009, viewed on 10 July 2021, https://cis-india.org/internet-governance/resources/it-procedure-and-safeguards-for-interception-monitoring-and-decryption-of-information-rules-2009.
[213] Section 2(d) of the Information Technology (Procedures and Safeguards for Interception, Monitoring and Decryption of Information) Rules 2009, viewed on 10 July 2021, https://cis-india.org/internet-governance/resources/it-procedure-and-safeguards-for-interception-monitoring-and-decryption-of-information-rules-2009.
[214] Section 3 of the Information Technology (Procedures and Safeguards for Interception, Monitoring and Decryption of Information) Rules 2009, viewed on 10 July 2021, https://cis-india.org/internet-governance/resources/it-procedure-and-safeguards-for-interception-monitoring-and-decryption-of-information-rules-2009.
[215] *Ibid.*
[216] Section 8 of the Information Technology (Procedures and Safeguards for Interception, Monitoring and Decryption of Information) Rules 2009, viewed on 10 July 2021, https://cis-india.org/internet-governance/resources/it-procedure-and-safeguards-for-interception-monitoring-and-decryption-of-information-rules-2009.
[217] Section 11 of the Information Technology (Procedures and Safeguards for Interception, Monitoring and Decryption of Information) Rules 2009, viewed on 10 July 2021, https://cis-india.org/internet-governance/resources/it-procedure-and-safeguards-for-interception-monitoring-and-decryption-of-information-rules-2009.
[218] Section 23 of the Information Technology (Procedures and Safeguards for Interception, Monitoring and Decryption of Information) Rules 2009, viewed on 10 July 2021, https://cis-india.org/internet-governance/resources/it-procedure-and-safeguards-for-interception-monitoring-and-decryption-of-information-rules-2009.
[219] Section 67C of the Information Technology Act 2000, viewed 26 July 2021, https://legislative.gov.in/sites/default/files/A2000-21_0.pdf.
[220] Section 25(2) of the Information Technology (Procedures and Safeguards for Interception, Monitoring and Decryption of Information) Rules 2009, viewed on 10 July 2021, https://cis-india.org/internet-governance/resources/it-procedure-and-safeguards-for-interception-monitoring-and-decryption-of-information-rules-2009.
[221] Section 25(1) of the Information Technology (Procedures and Safeguards for Interception, Monitoring and Decryption of Information) Rules 2009, viewed on 10 July 2021, https://cis-india.org/internet-governance/resources/it-procedure-and-safeguards-for-interception-monitoring-and-decryption-of-information-rules-2009.
[222] Section 28(5) of the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016, viewed on 10 July 2021, https://uidai.gov.in/images/targeted_delivery_of_financial_and_other_subsidies_benefits_and_services_13072016.pdf.

and confidentiality specifically applies to the use of core biometric information[223]. Such information cannot be shared with anyone for any reason, and cannot be used for any purpose other than the generation of Aadhaar numbers and consequent authentication under the act[224]. Further, identity information other than core biometric information may be shared in accordance with the provisions of the act and in accordance with the provisions of the regulations adopted by the government. After all, a wide level of discretion lies with the government in the decision of disclosing this type of information. Similarly, other data of the Aadhaar number holders, including the demographic information, may be published, displayed, or posted publicly for purposes specified in the regulations adopted by the government[225]. Finally, the principle of confidentiality enjoys a general exception, as any information, including biometrics, may be disclosed on the ground of national security, pursuant to a direction of an officer specially authorised by the government[226]. It specifies that the UIDAI may reveal identity information, authentication records, or any information, following a court order by a District Judge or higher. The Act also allows disclosures in the interest of national security, at the direction of a Joint Secretary to the Government of India or an officer of a higher rank, authorised for this purpose. The Act does not cover the issue of obtaining individuals' consent under these exceptions[227].

2.2.2.3 Oversight

i. The Review Committee (Telegraph Rules 1951)

The issues around the lack of an oversight mechanism in relation to governmental access to personal data are specifically addressed in the Report on Data Protection drafted by the Committee of Experts appointed by the government in 2017[228]. Due to the criticisms expressed by both the Committee and the Supreme Court of India in the *Puttaswamy* judgment[229], the necessity to build an oversight mechanism was an important point of attention in the drafting of the PDP Bill (See section 2.2.4: Upcoming changes in legislation).

Under the IT Act, a Review Committee in charge of reviewing interception orders can be set up[230]. The Review Committee consists of the Cabinet Secretary, the Secretary to the Government of India in the Department of Legal Affairs and the Secretary to the Government of India in the Department of Telecommunications[231]. The Report on Data Protection points out how the Committee is supposed to deal with an enormous number of orders every month, while only meeting once per month. It also underlines how the only review of the executive power is not in line with the review of legal systems of

[223] The core biometric information is defined, under Section 2(g) of the Aadhaar Act, as "finger prints, iris scan, or such other biological attribute of an individual as may be specified by regulations".
[224] Section 29(1) of the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016, viewed on 10 July 2021, https://uidai.gov.in/images/targeted_delivery_of_financial_and_other_subsidies_benefits_and_services_13072016.pdf.
[225] Section 29(4) of the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016, viewed on 10 July 2021, https://uidai.gov.in/images/targeted_delivery_of_financial_and_other_subsidies_benefits_and_services_13072016.pdf.
[226] Section 33(2) of the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016, viewed on 10 July 2021, https://uidai.gov.in/images/targeted_delivery_of_financial_and_other_subsidies_benefits_and_services_13072016.pdf.
[227] Ibid.
[228] Committee of Experts under the Chairmanship of Justice B.N. Srikrishna, "A free and fair digital economy. Protecting Privacy, empowering Indians", viewed on 26 July 2021, https://www.meity.gov.in/writereaddata/files/Data_Protection_Committee_Report.pdf.
[229] Supreme Court of India, 24 August 2017, WP(C) 494/2012, *Justice K. S. Puttaswamy v. Union of India*, https://scobserver-production.s3.amazonaws.com/uploads/case_document/document_upload/624/Right_to_Privacy__Puttaswamy_Judgment_.pdf.
[230] Section 22 of the Information Technology (Procedures and Safeguards for Interception, Monitoring, and Decryption of Information) Rules 2009, viewed on 10 July 2021, https://cis-india.org/internet-governance/resources/it-procedure-and-safeguards-for-interception-monitoring-and-decryption-of-information-rules-2009.
[231] Rule 419 of the Indian Telegraphs Rules 1951, viewed on 10 July 2021, https://cis-india.org/internet-governance/resources/rule-419-a-indian-telegraph-rules-1951.

other democratic nations. The lack of oversight, along with the issues around the independency of a governmental body overseeing governmental decisions, was also criticised by local experts[232].

ii. The Oversight Committee (the Aadhaar Act)

In relation to the Aadhaar Act, the *Puttaswamy* judgment can be mentioned once more. While the Supreme Court of India upheld its constitutionality, the notorious dissenting opinion of Justice Chandrauchaud expressed various concerns[233]. The distinguished justice argued that the UIDAI lacked an accountability mechanism. Also, the Aadhaar Act did not establish an independent monitoring authority to oversee the collection of personal data under the Aadhaar scheme[234]. However, according to Section 33 of the Aadhaar Act, every decision made by the government to disclose personal information on grounds of national security should be reviewed by an Oversight Committee. Such a committee should consist of the Cabinet Secretary, the Secretary to the government of India in the Department of Legal Affairs and the Secretary to the Government of India in the Department of Electronics and Information Technology[235]. Notwithstanding the indication of the Supreme Court of India to limit the discretional power of the executive authorities in disclosing such information and to add a judicial scrutiny in the context of the provision, these concerns were not addressed in the latest amendments to the Aadhaar Act[236].

2.2.3 Data subject rights

2.2.3.1 Conditions

i. The Information Technology Act

The Rules 2011 divided personal information for the IT Act into two broad categories, being 'personal data' and 'sensitive personal data'[237]. Personal data is defined as "*any information that relates to a natural person, which, either directly or indirectly, in combination with other information available or likely to be available with a body corporate, is capable of identifying such person*"[238]. Sensitive personal information is information relating to *(i) password; (ii) financial information such as bank account or credit card or debit card or other payment instrument details; (iii) physical, physiological and mental health condition; (iv) sexual orientation; (v) medical records and history; (vi) biometric information*[239].

In relation to the IT Act and Rules 2011, a "body corporate" or any person who processes personal information on behalf of the "body corporate" should provide a privacy policy[240]. Furthermore, the Rules

---

[232] According to an internal interview with a local expert.
[233] Supreme Court of India, 24 August 2017, WP(C) 494/2012, *Justice K. S. Puttaswamy v. Union of India*, https://scobserver-production.s3.amazonaws.com/uploads/case_document/document_upload/624/Right_to_Privacy__Puttaswamy_Judgment_.pdf.
[234] Chhugani, S., 2021, "India's Aadhaar card a violation of Indian citizen's right to privacy", Cardozo International & Comparative Law Review, 4(2), pp. 733-762, viewed on 21 July 2021.
[235] Section 33 of the Aadhaar (Targeted Delivery of Financial, and Other Subsidies, Benefits and Services) Act, 2016, viewed on 10 July 2021, https://uidai.gov.in/images/targeted_delivery_of_financial_and_other_subsidies_benefits_and_services_13072016.pdf.
[236] Software Freedom Law Center, 1 August 2019,. What has been changed in the Aadhaar Amendment Bill?, viewed on 15 July 2021, https://sflc.in/what-has-been-changed-aadhaar-amendment-bill.
[237] Art. 43(iii) of the Information Technology Act 2000, viewed 26 July 2021, https://legislative.gov.in/sites/default/files/A2000-21_0.pdf.
[238] Section 2(1)(i) of the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011, viewed on 6 June 2021, [भाग II- खण्ड 3(i)] भारत का राजपत्र : असाधारण 7 (meity.gov.in).
[239] Section 3 of the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011, viewed on 6 June 2021, [भाग II- खण्ड 3(i)] भारत का राजपत्र : असाधारण 7 (meity.gov.in).
[240] This privacy policy should serve to protect the personal information that is provided, and the provider of such information should be able to review the policy. The privacy policy is required to be made available on the website of the corporate body and should provide for: (i) clear and accessible statements relating to its practices and policies; (ii) the type of personal

2011 contain specific provisions regarding the collection of sensitive personal data by "body corporates" in India. When collecting sensitive data, the data collector must take reasonable steps to ensure that the data subject has knowledge of this collection[241]. A "body corporate" collecting sensitive personal data or information should keep the data subject informed about: (i) the fact that the information is being collected; (ii) the purpose; (iii) the intended recipients; and (iv) the name and address of the agency collecting and retaining the information[242]. The "body corporate" cannot keep sensitive personal data for longer than is required and has to ensure that reasonable security practices and procedures are applicable[243]. The data collector is not allowed to publish any sensitive personal data or information except when the prior written or electronic consent of the data subject is obtained[244]. A data subject can always withdraw the consent previously provided to the data collector[245]. Data subjects also have the right to access information[246]. Based on this right, the data subject can correct or update any inaccurate or incorrect information[247]. The rights established under the IT Act do not refer to governmental or public agencies, making it impossible to enforce rights against law enforcement/national security authorities[248]. However, Section 45 does foresee a residual penalty for those who contravene any rule or regulation for which no penalty has been separately provided. This imposes a residual responsibility on the State in a *pro forma* manner, as no trial will be held based on this provision.

As regards the "right to be forgotten", there is no mention of it under the Rules 2011 or in any other Indian laws, but it has been recognised in Indian case law, especially in relation to sexual offences against women, but it lacks an explicit provision in legislation[249]. As pointed out by Indian experts, the *Puttaswamy* judgment's influence was crucial in paving the way towards a wider recognition of this right in the Indian courts[250].

ii. The Aadhaar Act

The Aadhaar Act mentions similar elements as the Rules 2011. It states that individuals need to be informed about the manner in which the information shall be used and to whom the data might be shared[251]. In addition, the right to access information is also mentioned[252]. Interestingly, access to core

information or sensitive personal data or information that is being collected; (iii) the purpose of collecting and using of such information; (iv) the instances in which disclosure of such information may be made under the Rules; and (v) reasonable security practices and procedures required under the Rules.

[241] Section 5(3) of the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011, viewed on 6 June 2021, [भाग II- खण्ड 3(i)] भारत का राजपत्र : असाधारण 7 (meity.gov.in).

[242] *Ibid.*

[243] Section 5(4) of the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011, viewed on 6 June 2021, [भाग II- खण्ड 3(i)] भारत का राजपत्र : असाधारण 7 (meity.gov.in).

[244] Chowdhury, P., Thayil, K., 25 January 2021, Data Privacy in India, viewed 11 August 2021, https://www.mondaq.com/india/privacy/1005640/data-privacy-comparative-guide.

[245] *Ibid.*

[246] Section 5(6) of the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011, viewed on 7 June 2021, [भाग II- खण्ड 3(i)] भारत का राजपत्र : असाधारण 7 (meity.gov.in).

[247] *Ibid.*

[248] Section 43A IT Act.

[249] The Supreme Court of India has held that anonymity of victims must be maintained as far as possible in cases involving sexual offence (*State of Punjab vs Gurmit Singh*). The Karnataka High Court, in a recent decision, has recognised that certain information can be erased in sensitive cases involving rape, or affecting the modesty and reputation of the person concerned. However, other high courts have taken a different view in this regard. For example, the Gujarat High Court has rejected a plea to restrain public exhibition of a judgment on public sources (*Dharmraj Bhanushankar Dave v. State of Gujarat*).

[250] According to an internal interview with a local expert.

[251] Section 3(2) of Aadhaar Act 2016, viewed on 10 July 2021, https://uidai.gov.in/images/targeted_delivery_of_financial_and_other_subsidies_benefits_and_services_13072016.pdf.

[252] Section 28 of the Aadhaar Act 2016, viewed on 10 July 2021, https://uidai.gov.in/images/targeted_delivery_of_financial_and_other_subsidies_benefits_and_services_13072016.pdf.

biometric information[253] is excluded from this right[254]. Finally, information collected under the Aadhaar scheme may only be disclosed in case prior consent of the data subject is given[255].

2.2.3.2 Redress mechanisms

i. The Information Technology Act

The IT Act contains a chapter on punishments when personal data have been breached[256]. However, the only option to seek damages in case of a breach of personal data is provided by Section 43A. According to this provision, "body corporates" have an obligation to compensate the individuals when they fail to implement reasonable security practices and procedures in order to protect sensitive personal data, thus causing a wrongful loss or gain to any person[257]. As held before, the State and governmental bodies are not included in the definition of "body corporate". However, a form of liability of the State might be envisaged in a broad interpretation of Section 45, setting a residual penalty for whoever contravenes any rules or regulations of which no penalty has been separately provided. Nonetheless, the question of tortious acts committed by government servants in relation to their employment under the IT Act has not yet been addressed by the Indian judicial authorities[258].

Furthermore, the IT Act provides that an adjudicating officer, appointed by the Government, is competent in adjudicating any controversy arising under the provisions of the IT Act[259]. According to Indian experts, while the body is supposed to be independent, concerns arise from the fact that the appointment by the Government may impair such independency[260]. Besides, the IT Act states that no lawsuits, prosecution, or other legal proceeding may be initiated against the government or any person acting on behalf of it, when the action is carried out in good faith or intended to be done in pursuance of the IT Act or any regulation adopted on its basis[261]. Governmental officers generally benefit from this protection under Indian law, and the burden of proof in such cases lays on the petitioner, reducing the effectiveness of the redress mechanism[262].

ii. The Aadhaar Act

The Aadhaar Act also contains a chapter on offences and penalties[263]. Before the *Puttaswamy* judgment, the judicial authority could take cognisance of a complaint only where it was raised by UIDAI or an officer authorised by it[264]. However, after the judgment, the Aadhaar Act was amended to allow the

[253] Under the Aadhaar Act, "biometric information" is defined as photograph, finger print, iris scan, or any other biological attribute of an individual as specified in the regulations adopted by the Government to implement the legislation.
[254] Section 28 of Aadhaar Act 2016, viewed on 10 July 2021, https://uidai.gov.in/images/targeted_delivery_of_financial_and_other_subsidies_benefits_and_services_13072016.pdf.
[255] Section 29 of the Aadhaar Act 2016, viewed on 10 July 2021, https://uidai.gov.in/images/targeted_delivery_of_financial_and_other_subsidies_benefits_and_services_13072016.pdf.
[256] Chapter XI of the Information Technology Act 2000, viewed 26 July 2021, https://legislative.gov.in/sites/default/files/A2000-21_0.pdf.
[257] Section 43A Information Technology Act 2000, viewed 26 July 2021, https://legislative.gov.in/sites/default/files/A2000-21_0.pdf.
[258] Rajesh Bahuguna, R., 2020, Relevance of Distinction between Sovereign and Non-Sovereign Functions in governmental Liability In the Field of Cyber Torts: Indian Perspective, Journal of Critical Reviews, Vol. 7, Issue 14, pp. 4226-4230, viewed on 15 July 2021, http://www.jcreview.com/fulltext/197-1599744495.pdf.
[259] Section 46 of the Information Technology Act 2000, viewed 26 July 2021, https://legislative.gov.in/sites/default/files/A2000-21_0.pdf.
[260] According to an internal interview with a local expert.
[261] Section 84 of the Information Technology Act 2000, viewed 26 July 2021, https://legislative.gov.in/sites/default/files/A2000-21_0.pdf.
[262] According to an internal interview with a local expert.
[263] Chapter VII of Aadhaar Act 2016, viewed on 20 July 2021, https://uidai.gov.in/images/targeted_delivery_of_financial_and_other_subsidies_benefits_and_services_13072016.pdf.
[264] Software Freedom Law Center, 1 August 2019, What has been changed in the Aadhaar Amendment Bill?, viewed on 15 July 2021,, https://sflc.in/what-has-been-changed-aadhaar-amendment-bill.

courts to receive any kind of complaint made by Aadhaar number holders[265], including complaints against data processing carried out by public authorities, such as the UIDAI.

2.2.4 Upcoming changes in legislation

Besides the exceptions related to national security, the PDP Bill also provides exemptions from its provisions where personal data are processed in the context of prevention, detection and investigation and prosecution of any offence or any contravention under Indian law[266]. Moreover, a specific provision is dedicated to the processing of personal data of individuals located outside the territory of India. Based on the PDP Bill, the government will be able to exempt any data processor where the processing of personal data of subjects not within the territory of India is carried out pursuant to any contract stipulated between an individual or company incorporated outside India and any data processor incorporated under Indian law[267]. The extent of the provision remains unclear, due to the ongoing legislative process. However, the obligations on private entities to provide access to personal data at the request of the government are already extensive in Indian legislation. One potential effect of this provision could be the possibility for the government to exempt private entities from their obligations in respect of foreign data subjects in cases where the government requires access to their personal information. As there are no specific grounds needed for a government decision to provide for such exemptions, it could impact any foreigner whose personal data are processed by Indian entities.

In general, the exceptions provided by the proposed PDP Bill are in line with the already existing approach about government access to personal data, and have raised some criticism from digital rights' organisations, due to the vague phrasing and lack of more specific requirements and safeguards[268].

Furthermore, the PDP Bill contains a Chapter dedicated to the establishment of a Personal Data Protection Authority[269]. The Authority should have the function to protect the interests of data subjects and should help with the enforcement of the PDP Bill. However, the independence of the body to be created under the proposal has been put in question by fundamental rights' organisations and data protection experts[270]. This is based on the fact that the Selection Committee entitled to appoint the members of the Authority would include only members of the government, possibly infringing its independence[271].

2.2.5 Intermediary conclusion

The below grid summarises the content of the main Indian laws regulating the government access to personal data.

The first subsections investigate the situation in India regarding human rights and fundamental freedoms, in particular the right to privacy. It may be argued that the right to privacy was only recently recognised as a fundamental right in India, thanks to the Indian Supreme Court. In close connection, also the right to personal data has received more attention in recent times. However, the Indian government has a track record of infringing both rights extensively. As many human rights' organisations pointed out, the general situation regarding the right to privacy, as well as human rights

[265] *Ibid.*
[266] Section 36 of Personal Data Protection Bill, viewed on 27 July 2021, http://164.100.47.4/BillsTexts/LSBillTexts/Asintroduced/373_2019_LS_Eng.pdf.
[267] Section 37 of Personal Data Protection Bill, viewed on 27 July 2021, http://164.100.47.4/BillsTexts/LSBillTexts/Asintroduced/373_2019_LS_Eng.pdf.
[268] Centre for Internet and Society, 20 February 2020, An Annotated Version of the Personal Data Protection Bill 2019, viewed on 21 July of 2021, https://cis-india.org/accessibility/blog/annotated-ver-pdp-bill-2019.
[269] Chapter IX of the Personal Data Protection Bill, viewed on 27 July 2021, http://164.100.47.4/BillsTexts/LSBillTexts/Asintroduced/373_2019_LS_Eng.pdf.
[270] According to an internal interview with a local expert.
[271] Centre for Internet and Society, 20 February 2020, An Annotated Version of the Personal Data Protection Bill 2019, viewed on 21 July of 2021, https://cis-india.org/accessibility/blog/annotated-ver-pdp-bill-2019.

in general, may be largely improved.

The study of relevant Indian laws regulating purposes and conditions for the government access to personal data reveals that the existing guarantees of the right to privacy do not apply to the conduct of the State, leaving a worrying legislative vacuum in this area. The Indian legislation provides for widespread exemptions for governmental access to personal data with little or no guarantees for the data subjects. The grounds justifying such access to personal data are often very broad and vague concepts. In particular, the concept of 'national security', due to its broad phrasing and the absence of provisions narrowing down the meaning, leaves a significant level of discretion to the government in assessing when an intrusion into personal data is necessary to preserve national security interests. Moreover, the information to which the government may have access based on these exceptions includes all data stored on the Indian territory. In other words, the intrusion can also involve personal data of people in the EU. While the governmental access should meet some conditions, the oversight mechanisms on the enforcement of such conditions are not transparent and there is little evidence that they are fulfilled. As regards the bodies overseeing the respect of these conditions by the government, their independence from the executive is questionable.

In relation to data subjects' rights, it can be argued that their recognition is rather limited, due to the non-applicability to the government of most of the relevant provisions. In relation to remedies it can be held that, only in a few cases, it is possible for civilians to have access to a redress mechanism. In case of an infringement, the government itself remains mostly impenetrable. In the future, no additional protection for personal data seems to be upheld. While the draft PDP Bill explicitly recognises its applicability to the State, it also includes several exemptions from most of the provisions of the Bill, when governmental agencies process personal data for purposes related to national security or the fighting of crime.

Laws/ Features	Scope of Government Access	Oversight	Remedy/Data Subjects' Rights:
IT Act	Access to any computer source and collect any information contained in it, where it is deemed necessary or expedient to do so on various grounds related to interests of national security and the prevention of crimes. Allowance to the government to authorise any agency to monitor and collect any traffic data and information in any computer sources, based on the ground of enhancing national cybersecurity.	Internal oversight (Review Committee based on the Telegraph Rules 1951)	No rights against governmental body.
IT Rules 2021	Significant social media intermediaries primarily providing messaging services are obliged to provide the identity of the "first originator", namely the first person to send a message, upon judicial order, in the context of prevention, detection, investigation, prosecution or punishment of an offence related to national security, public order, international relations and sexually explicit material or child pornography.	Judicial decision	Right to access information: based on this right, the data subject can correct or update any inaccurate or incorrect information.

Aadhaar Act	Allowing government access to personal data in numerous circumstances. Numerous provisions empower the government to exercise a delegated power and adopt regulations to implement the Aadhaar Card Act.	Internal oversight (Oversight committee)	Possible to complain before court; Right of access to information (but biometric information excluded); Information collected under the Aadhaar scheme may only be disclosed if prior consent is given.
PDP Bill (future legislation)	Any governmental agency can be exempted from the application of all or any of the provisions of the Bill when processing personal data. The Bill also provides a general exemption to most of the provisions in the context of prevention, detection and investigation and prosecution of any offence or any contravention under Indian law.	External oversight (PDP Authority)	Compensation from data fiduciary or data processor. Explicit consent needed; Specific rights for children and employees; Right to data portability; Right to be forgotten.

2.3 RUSSIA

2.3.1 Rule of law, respect for human rights and fundamental freedoms

2.3.1.1 Context

The Russian Federation adopted its current Constitution in 1993[272], taking inspiration from Western Constitutional traditions and including internationally recognised democratic values and human rights[273]. According to the Constitution, Russia is "*a democratic federative law-governed state*", with its supreme value being the freedom and rights of individuals[274]. It grants basic human rights and freedoms to its citizens, which are recognised and guaranteed in line with "*universally recognised principles and norms of international law and this Constitution*"[275].

Nevertheless, in 2020, after the widely discussed *Zakharov v. Russia* case, the Constitution was amended, turning Russia further away from a democratic pathway[276]. The amendments removed the time-limit of the presidential term and, in general, further strengthened the position of the government. The independence of the judicial branch was also affected as the Constitutional Court (CC) lost its power to appoint the Head of the CC. Also, the Russian president now has the power to force the resignation of the president of the CC. Due to these changes, the highest court risks becoming more politicised. Simultaneously, the CC has been given power to evaluate whether judgments of international courts are

[272] Available at: https://web.archive.org/web/20130510161341/http://eng.Constitution.kremlin.ru/, viewed 26 July 2021.
[273] Kalinichenko, P., and Vladimirovich Kochenov, D., 2020, "Amendments to the 1993 Constitution of the Russian Federation Concerning International Law, *International Legal Materials* 60, no. 2, pp. 341–46, https://doi.org/10.1017/ilm.2021.10, p. 341.
[274] Articles 1 and 2 of the Russian Constitution.
[275] Article 17 of the Constitution.
[276] It can be noted, however, that much of the international criticism, case law and other non-democratic actions have taken place before the formal change of the Constitution.

compatible with the Russian Constitution[277]. De facto, this allows the CC to invalidate international judgments and hinder their implementation in Russia[278]. Nevertheless, the jurisprudence of the European Court of Human Rights (ECtHR) is not categorically dismissed and case law of the ECtHR remains to be cited by Russian courts and formally remains part of Russian law[279].

Currently, Articles 23 and 24 of the Russian Constitution guarantee the right to privacy and personal data. The relevant Articles of the Russian Constitution and of the EU-Charter are formulated using similar wording, but are not identical. Article 8 of the EU-Charter includes the supervision of independent authorities for compliance[280], whereas the Russian Constitution mentions the possibility to limit the right to privacy based on a "court order"[281]. In addition, the EU-Charter is more inclusive and comprehensive[282] whereas the Russian legislation is more detailed and potentially provides more possibilities for derogations by giving more autonomy to executive and security agencies[283].

In terms of international obligations, Russia has signed and ratified the European Convention of Human Rights (ECHR)[284], the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108), the updated Convention 108+ on protection of individuals with regard to the Processing of Personal Data (Convention 108+)[285] as well as the UN's International

[277] Article 104 of the Federal Law of December 14, 2015 N 7-FKK, https://rg.ru/2015/12/15/ks-site-dok.html, described also by Moyakine, E., and Tabachnik, A., 2021, "Struggling to Strike the Right Balance between Interests at Stake: The 'Yarovaya', 'Fake News' and 'Disrespect' Laws as Examples of Ill-Conceived Legislation in the Age of Modern Technology", *Computer Law & Security Review* 40, 105512, https://doi.org/10.1016/j.clsr.2020.105512, p.6.

[278] Russia has already done this with regard to the case Anchugov and Gladkov v Russia. The Constitutional Court in that case found that the implementation thereof was "impossible". As stated on p. 38-39 of judgement No. 12-П/2016: "*To recognize execution in accordance with the Constitution of the Russian Federation […], of the Judgment of the European Court of Human Rights of 4 July 2013 in the case of Anchugov and Gladkov v. Russia (applications nos. 11157/04 and 15162/05), […] contemplating making amendments to Russia's legislation (and thereby alteration of the judicial practice based on it), which would allow to restrict in electoral rights not all convicted persons serving a sentence in places of deprivation of liberty under a court sentence, – as* ***impossible****, so far as the prescription of Article 32 (Section 3) of the 39 Constitution of the Russian Federation, having* ***supremacy and supreme legal force*** *in Russia's legal system […]*". The enforcement is discussed in detail in an EJI blogpost, noting that the case was closed by the Council of Europe (CoE), but that questions remains regarding the actual enforcement of the judgement, see https://www.ejiltalk.org/case-closed-but-what-about-the-execution-of-the-judgment-the-closure-of-anchugov-and-gladkov-v-russia/; Anchugov and Gladkov v Russia, App no 11157/04 and 15162/05, ECtHR 4 July 2013, discussed in Kalinichenko and Kochenov, 2020, "Amendments to the 1993 Constitution of the Russian Federation Concerning International Law. See also: Judgment of 19 April 2016 No. 12-П/2016, http://www.ksrf.ru/en/Decision/Judgments/Documents/2016_April_19_12-P.pdf.

[279] Antonov, M., "Philosophy behind Human Rights: Valery Zorkin vs. the West?", in *Russia and the European Court of Human Rights*, ed. Mälksoo, L., and Benedek, W., 1st ed., Cambridge University Press, 2017, pp. 150–87, https://doi.org/10.1017/9781108235075.008, p. 166.

[280] Article 8(3) of the EU-Charter.

[281] Article 23 (2) of the Russian Constitution.

[282] Article 7 of the EU-Charter: "*Everyone has the right to respect for his or her private and family life, home and communications.*" and Article 8: "*Everyone has the right to the protection of personal data concerning him or her. 2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified. 3. Compliance with these rules shall be subject to control by an independent authority.*"

[283] Article 23 of the Russian Constitution: "1. *Everyone shall have the right to the inviolability of his (her) private life, personal and family privacy, and protection of his (her) honour and good name. 2. Everyone shall have the right to privacy of correspondence, of telephone conversations and of postal, telegraph and other communications. This right may be limited only on the basis of a court order.*" and Article 24: "*1. Collecting, keeping, using and disseminating information about the private life of a person shall not be permitted without his (her) consent. 2. State government bodies and local self-government bodies and their officials shall be obliged to provide everyone with access to documents and materials directly affecting his (her) rights and freedoms, unless otherwise envisaged by law.*"

[284] https://www.coe.int/en/web/conventions/search-on-states/-/conventions/treaty/005.

[285] The purpose of Convention 108(+) is to protect individuals "*with regard to their processing of personal data, thereby contributing to the protection of human rights and freedoms, and in particular the right to privacy.*". Article 1, Convention 108 +, Convention for the protection of individuals with regard to the processing of personal data, https://rm.coe.int/convention-108-convention-for-the-protection-of-individuals-with-regar/16808b36f1, https://www.coe.int/en/web/data-protection/russia.

Covenant on Civil and Political Rights[286]. By signing and ratifying the above documents, Russia commits to the protection of human rights, including the right to privacy and data protection in particular.

2.3.1.2 General findings of international organisations

In general, human rights are often violated in Russia[287]. Russia has the second most registered violations of human rights, with a total of 2 724 judgments of the ECtHR in the period 1959-2020[288]. An EU report highlighted the fact that although human and fundamental rights are enshrined in the Russian Constitution, a "*systematic crackdown*" thereof is the reality[289]. At the end of 2020, 13 650 applications against Russia to the ECtHR were pending[290]. Russia has been found to have violated the right to respect for private and family life 106 times by the ECtHR during the period 1959-2020[291]. In light of this, the EU has condemned the human rights' situation in Russia[292] and subjected the country to sanctions[293]. In February 2021, the European Council agreed on developing further restrictive measures in response to the serious violations of human rights in Russia[294].

In addition, the country is repeatedly criticised for not complying with the ECHR[295]. The cases *Zakharov v. Russia*[296] and *Shimovolos v. Russia*[297] can be discussed as two highly relevant examples of Russia's incompliance with international data protection law. Both cases show that the Russian data protection legislation did not meet the requirements of Article 8 of the ECHR.

In relation to the *Roman Zakharov v. Russia*[298] case, the applicant claimed that the mere existence of

[286] All Russia's commitments under the United Nation's Human Rights Treaties can be found though https://tbinternet.ohchr.org/_layouts/15/TreatyBodyExternal/Treaty.aspx?CountryID=144&Lang=EN, viewed 30 August 2021.

[287] Russia has been found to violate the right to life (Article 2 ECHR) 330 times, the right to inhumane or degrading treatment (Article 3 ECHR) 916 times, the right to liberty and security (Article. 5 ECHR) 1203 times, the right to a fair trial (Article 6 ECHR) 935 times, right to respect for private and family life (Article 8 ECHR) 244 times, freedom of expression (Article 10 ECHR) 95 times[287] and the right to an effective remedy (Article 13 ECHR) 660 times. Other important rights are for example freedom of thought, conscience and religion (Article 9 ECHR): 11 times, freedom of assembly and association (Article 11 ECHR): 68 times, prohibition of discrimination (Article 14 ECHR): 22 times. All statistics are from the CoE, viewed 11 May 2021, https://www.echr.coe.int/Documents/Stats_violation_1959_2020_ENG.pdf.

[288] See Statistics of the CoE: https://www.echr.coe.int/Documents/Stats_violation_1959_2020_ENG.pdf. As a comparison, Turkey has been found violating the ECHR in 3309 judgements during the same period.

[289] Joint Communication to the European Parliament, the European Council and the Council on EU-Russia relations – Push back, constrain and engage, JOIN(2021) 20 final, 16 June 2021, p. 2.

[290] CoE Statistics accessed 11.5.2021 via https://www.echr.coe.int/Documents/Stats_pending_2021_BIL.pdf

[291] See statistics of the Council of Europe, accessed via https://www.echr.coe.int/Documents/Stats_violation_1959_2020_ENG.pdf on 15.6.2021.

[292] Joint Communication to the European Parliament, the European Council and the Council on EU-Russia relations – Push back, constrain and engage, JOIN(2021) 20 final, 16 June 2021, p 10.

[293] Sanctions imposed as a response to the annexation of Crimea, as described: https://www.consilium.europa.eu/en/policies/sanctions/ukraine-crisis/, extended 21/6/2021, see Council of the European Union press release, https://www.consilium.europa.eu/en/press/press-releases/2021/06/21/russia-s-illegal-annexation-of-crimea-and-sevastopol-council-renews-sanctions-for-a-further-year/?utm_source=dsms-auto&utm_medium=email&utm_campaign=Russia%27s+illegal+annexation+of+Crimea+and+Sevastopol%3a+Council+renews+sanctions+for+a+further+year.

[294] Outcome of the Council Meeting on Foreign Affairs, 22 February 2021, p. 5, viewed 11 May 2021, https://data.consilium.europa.eu/doc/document/ST-6295-2021-INIT/en/pdf.

[295] Shcherbovich, A., "Data Protection and Cybersecurity Legislation of the Russian Federation in the Context of the 'Sovereignization' of the Internet in Russia", in *CyberBRICS*, ed. Belli, L., Cham: Springer International Publishing, 2021, pp. 67–131, https://doi.org/10.1007/978-3-030-56405-6_3.

[296] ECtHR, *Roman Zakharov v. Russia*, App. No. 47143/06, 4 December 2015.

[297] ECtHR, *Shimovolos v. Russia*, App. No. 30194/09.

[298] ECtHR 4 December 2015, App. No. 47143/06, *Roman Zakharov v. Russia*, discussed in e.g. Cole, M. D., and Vandendriessche, A., 2016, "From Digital Rights Ireland and Schrems in Luxembourg to Zakharov and Szabó/Vissy in Strasbourg", *European Data Protection Law Review* 2, vol. 1, pp. 121–29, https://doi.org/10.21552/EDPL/2016/1/18; de Hert and Bocos, "Case of Roman Zakharov v. Russia: The Strasbourg Follow up to the Luxembourg Court's Schrems Judgment," *Strasbourg Observers*, 23 December 2015 г., https://strasbourgobservers.com/2015/12/23/case-of-roman-zakharov-v-russia-

Russian legislation allowing interception of mobile-phone communications and the risk of being subject to interception by Russian public authorities interfered with his rights[299]. Although the right to privacy can be limited, the ECtHR confirmed that, in this case, the legislation did constitute secret surveillance under which any person using mobile-telephone services of Russian providers could have his/her mobile-telephone communications intercepted. This without ever being notified of the surveillance[300]. Furthermore, the ECtHR held that no effective remedies were provided[301]. Also, the Operational Search Activities Act (OSAA) allowed courts to grant interceptions in a general manner, not specifying the specific persons or telephone numbers to be intercepted[302]. In urgent cases, interception was possible without prior authorisation for up to 48 hours[303]. The ECtHR also found further shortcomings in the supervisory arrangements[304].

In relation to the *Shimovolos v. Russia* case, the applicant had been registered as a "human rights activist" in the Russian Surveillance Database[305]. As a result, the applicant became subject to identity checks and questioning during travels[306]. In this case, the ECtHR concluded that registering names in the Surveillance Database, collecting information about a person's movements and storing this data concerned an interference with the right to private life[307]. The ECtHR also concluded that the Russian legislation creating the Surveillance Database, and the maintenance thereof was not publicly accessible. In addition, no safeguards against abuse were available[308].

In 2014, the UN General Assembly published the report of the Special Rapporteur on the independence of judges and lawyers[309]. In relation to Russia, the report raised concerns on "*improper influence, interference and pressure*" being put on the judiciary, affecting the role of the courts to fulfil their "*role as guardians of the rule of law*"[310]. Concerns also related to attempts made by State authorities and private actors to control the judicial processes[311], the appointment procedures and the independence of the judicial[312].

Further, in 2015, the United Nations Human Rights Council (HRC) adopted Concluding observations on the enjoyment of human rights in Russia[313]. The HRC's observations comprise a set of concerns related to, for example, discrimination, racial profiling (including e.g. harassment, arrests, detentions and physical abuse)[314], the independence of the judiciary[315] and harassment, violence and killing of

---

the-strasbourg-follow-up-to-the-luxembourg-courts-schrems-judgment/. See also The Applicability of Schrems Principles to the Member States: National Security and Data Protection within the EU Context, *Practical Law*; Secret Surveillance of Mobile Telephone Communications, Europan Human Rights Law Review, 2016, 2, 201-205.

[299] *Roman Zakharov v. Russia*, para. 163.

[300] *Ibid.*, para. 175.

[301] *Ibid.*, para. 286-300 and 176.

[302] *Ibid.*, para. 265.

[303] *Ibid.*, para. 265.

[304] *Ibid.*, para. 285.

[305] *Shimovolos v. Russia*, App. No. 30194/09, para. 6.

[306] *Ibid.*, para. 11-16.

[307] *Ibid.*, para. 66.

[308] *Ibid.*, para. 68-71.

[309] Report of the Special Rapporteur on the independence of judges and lawyers - Mission to the Russian Federation (A/HRC/26/32/Add.1), https://www.ohchr.org/EN/Countries/ENACARegion/Pages/RUIndex.aspx. It should be noted that it is not useful nor relevant to recall all the concerns raised by the Special Rapporteur. Therefore, only those which are considered relevant for the purpose of this report are raised.

[310] Report of the Special Rapporteur on the independence of judges and lawyers - Mission to the Russian Federation (A/HRC/26/32/Add.1), section A, para. 14, https://www.ohchr.org/EN/Countries/ENACARegion/Pages/RUIndex.aspx.

[311] *Ibid*, para. 15.

[312] *Ibid*, para. 19-20 in particular.

[313] UN Human Rights Committee, Concluding observations on the seventh periodic report of the Russian Federation, CCPR/C/RUS/CO/7, viewed 15 June 2021, https://tbinternet.ohchr.org/_layouts/15/treatybodyexternal/Download.aspx?symbolno=CCPR/C/RUS/CO/7&Lang=En.

[314] *Ibid*, point 9.

[315] *Ibid*, point 17.

lawyers, journalists, human rights defenders and opposition politicians[316], developments affecting the freedom of expression and dissenting political opinions[317] and freedom of association[318]. More recently, during the 46th session of the HRC, a statement of 84 different Russian and international organisations was issued[319]. It urged the members of the HRC to take action against the human rights' situation in Russia[320]. The statement also criticises the Foreign Agents Law[321], which requires organisations engaging in political activity and receiving funding from abroad to register as foreign agents. According to the statement, the law defines "political activity" broadly, which allows the authorities to identify human rights' organisations, media and individual journalists and bloggers as foreign agents[322].

In addition, other international organisations such as Human Rights Watch[323], Human Rights House Foundation[324] and Amnesty International[325] noted the declination of freedom of expression online and offline, as well as media freedoms[326]. Already in 2020, Human Rights Watch warned about a Russian bill which would give the authorities the power to block websites which filter Russian state media content, such as Facebook, Twitter and Youtube[327]. The organisation held that the law was used to obstruct human rights' organisations, or so called "undesirable" organisations[328]. Similar reports on the use of legislation to cause disturbance to human rights' organisations are also published by Amnesty International[329]. In its Annual Report for 2020, Amnesty International referred to the so-called "fake news" act, which criminalises spreading (knowingly) false information about circumstances which poses a threat to the lives and security of individuals, or about the government's actions to protect the population[330]. However, this law was used against journalists, civil activists and bloggers[331].

When it comes to organisations specialised in privacy and data protection rights, Privacy International has raised concerns about surveillance tendencies in Russia, especially in relation to COVID-19 tracking and facial recognition[332]. Finally, the organisation Agora noted that Russian policing institutions'

[316] *Ibid*, point 18.
[317] *Ibid*, point 19.
[318] *Ibid*, point 22.
[319] See for example https://humanrightshouse.org/statements/hrc46-statement-on-russia/.
[320] See https://humanrightshouse.org/statements/human-rights-council-members-must-strongly-denounce-russias-domestic-human-rights-violations/.
[321] Federal Law No. 481-FZ, Foreign Agents Law or 31.12.2020, available at http://publication.pravo.gov.ru/Document/View/0001202012300001 (in Russian).
[322] See Human Rights House "Human Rights Council Members must strongly denounce Russia's domestic human rights violations", 10 February 2021, viewed 21 June 2021, https://humanrightshouse.org/statements/human-rights-council-members-must-strongly-denounce-russias-domestic-human-rights-violations/.
[323] See for example Human Rights Watch, "Online and On All Fronts Russia's Assault on Freedom of Expression", viewed 21 June 2021, https://www.hrw.org/report/2017/07/18/online-and-all-fronts/russias-assault-freedom-expression and Human Rights Watch "Russia Closing Down Media Freedoms", published 29 April 2021, viewed 21 June 2021, https://www.hrw.org/news/2021/04/29/russia-closing-down-media-freedoms.
[324] Human Rights House Foundation, "Russia: Telegram block leads to widespread assault on freedom of expression online", viewed 21 June 2021, https://humanrightshouse.org/letters-of-concern/russia-telegram-block-leads-widespread-assault-freedom-expression-online/, including the signature of 26 human rights organisations.
[325] Amnesty International, "Unfair game: persecution of human rights defenders in Russia intensifies", 2019, viewed 21 June 2021, https://www.amnesty.org/download/Documents/EUR4609502019ENGLISH.pdf.
[326] See for example Human Rights Watch, "Online and On All Fronts Russia's Assault on Freedom of Expression", viewed 21 June 2021, https://www.hrw.org/report/2017/07/18/online-and-all-fronts/russias-assault-freedom-expression and Human Rights Watch "Russia Closing Down Media Freedoms", published 29 April 2021, viewed 21 June 2021, https://www.hrw.org/news/2021/04/29/russia-closing-down-media-freedoms.
[327] Human Rights Watch 2020, https://www.hrw.org/news/2020/11/23/new-law-would-expand-internet-censorship-russia.
[328] Human Rights Watch, 5 May 2021, viewed 21 June 2021, https://www.hrw.org/news/2021/05/05/russia-withdraw-new-batch-oppressive-laws.
[329] Amnesty International, "Unfair game: persecution of human rights defenders in Russia intensifies", 2019, viewed 21 June 2021, https://www.amnesty.org/download/Documents/EUR4609502019ENGLISH.pdf.
[330] Amnesty International - Annual report 2020, https://www.amnesty.org/en/countries/europe-and-central-asia/russian-federation/report-russian-federation/.
[331] *Ibid.*
[332] Privacy International, search on Russia, https://privacyinternational.org/search?keywords=russia&page=1; Privacy International on surveillance, https://privacyinternational.org/advocacy/3218/responding-global-proliferation-surveillance-

practices include the collection of online information on activists and protesters, information which is subsequently referred to in public documents. This is also referred to as "*online surveillance*"[333].

2.3.2 Government access to personal data

2.3.2.1 Purposes

i. General

Different grounds exist for the access to personal data by Russian authorities. These include cases of personal data processing carried out for the purposes of defence, security, countering terrorism, transport security, combating corruption, operational investigative activities, enforcement proceedings, and the penal legislation of the Russian Federation. Russian authorities are also allowed to process special categories of personal data (ethnicity, race, political and religious beliefs, sexual life) for one of the above-mentioned purposes. Another general policy objective which has been given to justify intrusive provisions, is the digital sovereignty of Russia[334].

ii. The Personal Data Law

The Federal Law No. 152-FZ (the Personal Data Law)[335] is the principal data protection law in Russia. The wording of the Personal Data Law is similar to that of the GDPR. Personal Data Law is also applicable to the processing of personal data for law enforcement purposes. 'Personal data' is defined as any information related to a directly or indirectly identified or identifiable natural person (data subject)[336]. An operator is a state body, a municipal body, a legal entity or an individual, independently or jointly with other persons organising and/or carrying out the processing of personal data, determining the purposes of processing, the composition of personal data to be processed, and the actions performed with personal data[337].

According to the law, processing of personal data is any action or set of actions performed with the use of automation tools or without the use of such tools with personal data, including collection, recording, systematisation, accumulation, storage, clarification (update, change), extraction, use, transfer (distribution, provision, access), depersonalisation, blocking, deletion, destruction of personal data[338].

The data subject decides whether or not to provide consent to the processing of their personal data. However, the Personal Data Law contains a provision on data subjects' obligatory consent to processing of their personal data in order to "protect the foundations of the constitutional order, morality, health, rights and legitimate interests of others, to ensure the defence of the country and the security of the State"[339].

State bodies, the Bank of Russia and local self-government bodies may, within the limits of their powers, adopt normative legal acts and regulations on certain issues related to the processing of personal data. Such acts can establish restrictions on the activities of operators or can impose obligations on operators not provided for by federal laws. However, such acts cannot contain provisions restricting the rights of

technology-our-strategy; Privacy International on Telegram and censorship, https://privacyinternational.org/long-read/2026/telegram-russia-compliance-and-complicity-russian-governments-attack-privacy.

[333] https://files.inclo.net/content/pdf/20/spying-on-dissent-Report_EN.pdf.

[334] Shcherbovich, "Data Protection and Cybersecurity Legislation of the Russian Federation in the Context of the 'Sovereignization' of the Internet in Russia", p. 67-68.

[335] Federal Law of 27 July 2006 N 152-FZ on personal data, accessed 14.9.2021, https://pd.rkn.gov.ru/authority/p146/p164/.

[336] Article 3(1) of the Personal Data Law.

[337] Article 3(2) of the Personal Data Law.

[338] Article 3(3) of the Personal Data Law.

[339] Article 9 of the Personal Data Law.

personal data subjects. Also, such acts are subject to official publication[340]. To be complete, it can be held that the Personal Data Law does not apply to[341]:

- The processing of personal data by individuals solely for personal and family needs, if this does not violate the rights of subjects of personal data;
- The organisation of storage, acquisition, accounting and use of documents containing personal data from the Archival Fund of the Russian Federation and other archival documents in accordance with the legislation on archiving in the Russian Federation;
- The processing of personal data classified in the prescribed manner as information constituting a state secret.

iii. The Data Protection Act

The Russian Federal Law No. 149-FZ on Information, information technologies and data protection (Data Protection Act)[342] regulates legal relations arising from (i) the exercise of the right to search, receive, transfer, produce and disseminate information; (ii) the use of information technology; (iii) the protection of information. The Data Protection Act requires that controllers notify the *Roskomnadzor*, the Russian federal watchdog responsible for monitoring, controlling and regulating mass media, communications, information technology, and processing of personal data, prior to the processing of personal data.

iv. The Data Localisation Law

One important component affecting the level of data protection in Russia relates to provisions on localisation of personal data. The so-called Data Localisation Law (Law No. 242-FZ)[343] is a federal law, which amended the Data Protection Act[344]. The core of this amendment consisted of obligations for operators to make sure that recoding, systematisation, accumulation, storage, refining and retrieving of personal data would be carried out on the territory of the Russian Federation. The Data Localisation Law is a good example of a piece of legislation, which is introduced with reference to the rights and safety of individuals (and national security) as its objective, but which has extensive effects on privacy and transfers of personal data.

The geographical dimension of the law prescribes that the relevant databases for the processing shall be located on Russian territory. Further, whereas the retention obligation concerns personal data of Russian citizens, it targets both Russian companies which may be storing data abroad, as well as foreign operators which are active in Russia, e.g., by providing services to Russian customers. Operators must ensure that information on the physical localisation of the servers are available.

The law is based on the motivation that data relating to internet activities of individuals with foreign services, where the data is processed outside Russia, could present a threat to individuals and to national

[340] See for example: Directive of the Bank of Russia No. 3889-U "On identifying threats to the security of personal data that are relevant when processing personal data in personal data information systems"; Order of the Federal Security Service No. 378 "On approval of the Composition and content of organisational and technical measures to ensure the security of personal data during their processing in information systems of personal data using cryptographic information protection tools necessary to fulfil the requirements established by the Government of the Russian Federation for the protection of personal data for each of the security levels".
[341] Article 1(2) of the Personal Data Law.
[342] Federal Law No. 149-FZ of July 27,2006 on information, information technologies and information protection, https://398-fz.rkn.gov.ru/docs/149-FZ.pdf (in Russian).
[343] Federal Law No. 242-FZ of July 21, 2014 on Amending Some Legislative Acts of the Russian Federation in as Much as It Concerns Updating the Procedure for Personal Data Processing in Information-Telecommunication Networks, https://pd.rkn.gov.ru/authority/p146/p191/ (English translation).
[344] Article 1 of Federal Law No. 242-FZ of July 21, 2014 on Amending Some Legislative Acts of the Russian Federation. Also described in Shcherbovich, "Data Protection and Cybersecurity Legislation of the Russian Federation in the Context of the 'Sovereignization' of the Internet in Russia.", pp. 68-71.

security[345]. The described provisions also refer to the need to protect data subjects. Nevertheless, the law may be considered to be restricting the free flow and transfer of personal data outside Russia.

v. The federal law on counter-terrorism

In March 2006, Federal Law No. 35-FZ on counter-terrorism was adopted. The law was amended in 2016 and is often referred to as the "*Yarovaya* law" or "*Yarovaya* package"[346]. The "package" consisted of two laws, which amended the Law on combating terrorism and the Criminal Code of Russian Federation, respectively. The main amendments included the introduction of three new types of criminal offences in the Criminal Code, being (i) failure to report a terrorist crime, (ii) assistance to extremist activities and (iii) the commission of an act of international terrorism. In addition, the amendments created an obligation for telecom operators to store calls and messages (including pictures, videos and audio recordings) of subscribers for a period of up to six months. Also, telecom operators were obliged to store 'information about subscribers' messages' for a period of up to three years and one year for Internet-based messenger services ('organisers of data distributions on the Internet'). Further, telecom operators now have to store extensive information on users such as mobile phone number, IMSI, CDMA, login, IP address, email, PIN code, full name, national ID data[347]. Finally, internet-based messenger service operators are obliged to provide data on decoding (unencrypting) users' messages to local divisions of Federal Security Service of Russian Federation (FSB).

By a Decree of the Ministry of Communications in October 2018[348], a requirement was introduced, requiring data distribution organisers (operators) to provide the technical means to allow search, processing, and transfer of stored data to the FSB. *Roskomnadzor* holds a list of the data distribution organisers, including among others, email services, and Russian social media operators[349]. If operators do not comply with this requirement, their services can be blocked in Russia. This can be compared to requirements of access schemes allowing access to personal data for intelligence agencies in the EU. In Russia, a telecom or internet operator is obliged by law to install software and hardware (also called SORM, System for Operative Investigative Activities) which allows the FSB to simply enter the system and access the personal data in the system. Since the operator does not need to be notified, a court order regarding the access is only visible for the relevant FSB agents and their supervision[350]. Scholars also stress that the intrusiveness of this system is further enhanced by the "subordination of courts" to services like the FSB and the rule of law issues in Russia[351].

If considering the functioning of the *Yarovaya* law, the interference with fundamental rights does not seem to be limited to what is strictly necessary, especially in light of the *Zakharov*-criteria of the ECtHR. The law has been challenged by the popular communication services provider Telegram in a renowned case, where implementation of the *Yarovaya* law was refused, as a protest and attempt to protect the rights of its users[352]. Telegram was fined for its refusal to hand over encryption key to the FSB and in April 2018 a decision was adopted authorising *Roskomnadzor* to block the services of Telegram. Further, Telegram lost the subsequent appeal in the Supreme Court of Russia in 2019. Eventually *Roskomnadzor*

[345] Shcherbovich, p. 68.
[346] Federal law of 6 July 2016 No. 374-Fz, http://kremlin.ru/acts/bank/41108/page/1.
[347] Order of Ministry of Digital Development, Communications and Mass Media of the Russian Federation, 29 October 2018, N 573.
[348] Order of Ministry of Digital Development, Communications and Mass Media of the Russian Federation dated 29.10.2018 N 573.
[349] Described by Gurkov, Alexander, in "Personal Data Protection in Russia," in The Palgrave Handbook of Digital Russia Studies, ed. Gritsenko, Daria, Mariëlle Wijermars, and Mikhail Kopotev (Cham: Springer International Publishing, 2021) p. 103.
[350]Moyakine, E. and A. Tabachnik, "Struggling to Strike the Right Balance between Interests at Stake: The 'Yarovaya', 'Fake News' and 'Disrespect' Laws as Examples of Ill-Conceived Legislation in the Age of Modern Technology," Computer Law & Security Review 40 (1 April 2021) p. 5.
[351] Moyakine and Tabachnik. p. 5.
[352] As described by HRW,"Telegram Loses Free Expression Battle to Russian Authorities", viewed 31 August 2021, https://www.hrw.org/news/2018/04/13/telegram-loses-free-expression-battle-russian-authorities.

allowed the functioning of Telegram in Russia, but the decision of Tagansky district court formally remains in force. Nevertheless, it should be noted, that the *Roskmonadzor* has not been able to enforce the legislation effectively in relation to a handful of West-based companies such as Google, Twitter and Telegram[353].

2.3.2.2 Conditions

The FSB has a wide range of rules and criterions establishing government access to personal data, as has been explained above with regard to the *Yarovaya* law. However, the Russian access regime seems to be lacking specific and transparent criteria, which would fulfil the criterion of necessity and proportionality as described in the EU-Charter[354]. As has been explained above, based on the *Yarovaya* law, operators are obliged to install software which allows the FSB to directly access the data stored by the operators. This access is direct and general, as it is not limited to certain data. This can be done without notifying the data controller or the data subject. Even though a court order system exists, a court order will only be visible to the FSB. The fact that not the data controller nor the data subject will be notified, deprives those of their right to challenge the lawfulness of the access. This lack of restrictions, oversight and possibility for redress do not seem to fulfil the criteria set in *Zakharov*, nor by the EU-Charter.

In 2019, the Supreme Court of Russia confirmed the legality of permanent remote access for the FSB and Ministry of Internal Affairs of Russia to the databases of communications providers containing personal data[355]. Such access does not require an additional court order or other form of authorisation.

In June 2021, the *Gosudarstvennaia Duma* (Parliament) amended the Law "On Communications" of the Russian Federation to allow the *Roskomnadzor* to directly access personal data stored in the databases of communications providers without a court order[356]. The system of court oversight for such access existed prior to the June 2021 amendments.

The Federal Service for Technical and Export Control (FSTEC) is an executive agency dealing with counter-intelligence and information security. While the FSTEC is involved in developing standards and rules for information protection using encryption, the FSB stores the encryption keys used by communication service providers to encrypt messages and personal data.

2.3.2.3 Oversight

Both the *Roskomnadzor* and the FSB ensure, organise and exercise state control and supervision over the compliance of the processing of personal data with the requirements of the Personal Data Law and regulatory legal acts adopted in accordance with it. The Personal Data Law lists the following supervisory functions of the *Roskomnadzor*:

- Handle requests from individuals or legal entities in order to obtain information necessary for the exercise of their powers, and receive such information free of charge;
- Carry out verification of the information contained in the notification on the processing of personal data, or ask other state bodies to carry out such verification within the limits of their authority;
- Require the operators to clarify, block or destroy inaccurate or illegally obtained personal data;
- Restrict access to information processed in violation of the legislation of the Russian Federation

[353] *Ibid*., p. 9; Zhuravlev, M. S. and Brazhnik, T. A., 2018, "Russian Data Retention Requirements: Obligation to Store the Content of Communications", *Computer Law & Security Review* 34, no. 3, pp. 496–507, p. 496 and 497.
[354] Moyakine and Tabachnik, p. 4.
[355] Decision of the Supreme Court of the Russian Federation of December 19, 2018 N АКПИ18-1109, accessed via: https://vsrf.ru/lk/practice/cases/10132425
[356] Roskomnadzor will gain access to personal data of subscribers without a court decision, 17 June 2021, accessed via: https://pravo.ru/news/232589/.

in the field of personal data;
- File a lawsuit in the court in defence of the rights of subjects of personal data, including in defence of the rights of an indefinite circle of persons, and represent the interests of subjects of personal data in court;
- Forward the information on the use of encryption protocols and encryption keys to the FSB;
- Provide material to the prosecutor's office, other law enforcement agencies to resolve the issue of initiating criminal cases on the basis of crimes related to the violation of the rights of subjects of personal data;
- Submit to the Government of the Russian Federation proposals on improving the legal regulation of the protection of the rights of subjects of personal data;
- Issue administrative fines to the persons guilty of violating the Personal Data Law.

The remedial or corrective powers of the *Roskomnadzor* in respect of public authorities are not explicitly stated among its functions. In practice, the *Roskomnadzor* issues fines or warnings exclusively to private entities and natural persons[357]. In its 2020 report, the *Roskomnadzor* reported reviewing 24 complaints about the quality of State services in the fields of media and communications.

The *Roskomnadzor* is subordinate to the Ministry of Digital Affairs of Russia. It is responsible for issuing authorisations for the legal functioning of media in Russia. Previously, it refused to issue such authorisations to media affiliated with Russian opposition politicians Alexey Navalny and Dmitry Gudkov[358]. The *Roskomnadzor* is authorised to block websites without a court order and has previously blocked or threatened to block [redacted]. Most of the restrictions were later lifted. The *Roskomnadzor* also demanded that Google and YouTube censor certain content related to Russian opposition leader Alexey Navalny[359].

2.3.2.4 Retention of personal data

The Personal Data Law states that personal data must be stored no longer than required for the purpose of processing personal data, unless otherwise stated by law, or by a contract in the case of a commercial relationship between the parties. If the purpose of processing personal data is achieved, the controller is obliged to immediately stop processing and destroy the personal data no later than three days after achieving the purpose[360]. According to the Order of the Federal Archive Agency of the Russian Federation No. 236, some documents containing the personal data of employees must be stored by the respective employer for up to 75 years, depending on the type of document[361].

[357] Report on the implementation of the plan and performance indicators of Roskomnadzor in 2020, accessed via: https://rkn.gov.ru/docs/doc_3158.pdf.
[358] Roskomnadzor did not issue a licence to register media outlets to Dmitry Gudkov, FBK and Open Media – Novaya Gazeta, 24 April 2019, accessed via: https://novayagazeta.ru/news/2019/04/24/151174-roskomnadzor-ne-vydal-litsenziyu-na-registratsiyu-smi-dmitriyu-gudkovu-fbk-i-otkrytym-media (In Russian).
[359] Google first lawsuit against Roskomnadzor – Novaya Gazeta, 24 May 2021, accessed via: https://novayagazeta.ru/articles/2021/05/24/google-vpervye-podala-isk-k-roskomnadzoru?utm_source=tw&utm_medium=novaya&utm_campaign=google-llc-vpervye-podala-isk-k-roskomna (In Russian).
360 Article 21(4) of the Personal Data Law.
361 Order of the Federal Archive Agency of the Russian Federation No. 236 "The list of standard administrative archival documents generated in the course of the activities of state bodies, local authorities and organizations, indicating the terms of their storage".

2.3.3 Data subject rights

2.3.3.1 Conditions

i. General

In Russia, the Personal Data Law[362] and the Data Protection Act[363] provide principles and obligations intended to protect the personal data of data subjects. These will be described in the following sections. In general, data subjects have the right to demand the operator for information of their personal data. The information on processing personal data has to be provided to the data subject or their representative by the operator upon receiving a request from the subject of personal data or their representative. The request must contain the ID number of the data subject or of their representative, proof of relations with the operator (e.g. contract), or information otherwise confirming the fact of personal data processed by the operator. The request can be sent in the form of an electronic document in accordance with the legislation of the Russian Federation. The right of the data subjects to access their personal data may be limited if:

- the processing of personal data, including personal data obtained as a result of investigative, counterintelligence and intelligence activities, is carried out for the purpose of national defence, state security and law enforcement;
- the processing of personal data is carried out by the bodies that detained the subject of personal data on suspicion of committing a crime, or charged the subject of personal data in a criminal case, or applied a preventive measure to the subject of personal data before filing charges, with the exception of those provided for by the criminal procedural legislation of the Russian Federation cases when it is allowed to familiarise the suspect or the accused with such personal data;
- the processing of personal data is carried out in accordance with the legislation on combating the legalisation (laundering) of funds obtained through crime and the financing of terrorism;
- the access of the personal data subject to their personal data violates the rights and legitimate interests of third parties;
- the processing of personal data is carried out in the cases provided for by the legislation of the Russian Federation on transport security, in order to ensure the stable and safe operation of the transport complex, to protect the interests of the individual, society and the state in the field of the transport complex from acts of unlawful interference.

In addition, the data subject has the right to ask for the blocking or destruction of personal data if the personal data is incomplete, outdated, inaccurate, illegally obtained or not necessary for the stated purpose of processing, as well as to take measures provided for by law to protect their rights.

ii. The Personal Data Law

In relation to the Personal Data Law[364], there are several principles protecting the rights of data subjects. First of all, it is held that the processing of personal data must be carried out on a legal and fair basis[365]. Furthermore, the processing of personal data should be limited to the achievement of specific, predetermined and legitimate goals[366]. Processing of personal data that is incompatible with the purposes

[362] Federal Law of 27 July 2006 N 152-FZ on Personal Data, viewed 31 August 2021, https://pd.rkn.gov.ru/authority/p146/p164/ (English translation).
[363] Federal Law No. 149-FZ of July 27,2006 on information, information technologies and information protection, https://398-fz.rkn.gov.ru/docs/149-FZ.pdf (in Russian).
[364] Federal Law of 27 July 2006 N 152-FZ on Personal Data, viewed 31 August 2021, https://pd.rkn.gov.ru/authority/p146/p164/ (English translation).
[365] Article 5(1) of the Personal Data Law.
[366] Article 5(2) and (5) of the Personal Data Law.

of collecting personal data is not allowed[367]. In addition, the content and volume of processed personal data must comply with the stated processing objectives. The processed personal data should not be redundant in relation to the stated purposes of their processing. Further, the operator must take the necessary measures to remove or clarify incomplete or inaccurate data[368]. It is also held that the storage of personal data must be carried out in a form that makes it possible to determine the subject of personal data. In addition, the processed data are subject to destruction or depersonalisation upon achievement of the processing goals or in case of loss of the need to achieve these goals, unless otherwise provided by federal law[369].

The Personal Data Law also provides extensive legislation with regard to the conditions of processing personal data[370], such as the consent of the data subject[371] or several legal bases related to state authorities' processing of personal data. These are for example: (i) processing of personal data for achieving purposes stipulated by a law; (ii) processing of personal data for exercise and fulfilment of functions, powers and obligations imposed on operators by the Russian Federation law[372]; (iii) processing of personal data for the administration or enforcement of judicial acts[373]; and (iv) processing of personal data subject to publication or compulsory disclosure in accordance with federal laws[374].

The Personal Data Law also requires consent for processing of special categories of personal data (e.g. political and religious views, ethnic and racial background, sexual life) as a principle[375], the principle is, nevertheless subject to a list of exceptions[376] related to the public availability of the information, the necessity of processing for health, pension and insurance reasons. Interesting exceptions also allow processing of personal data of special categories if it is "*necessary in order to enable the rights of the personal data subject or of third parties to be established or exercised, and in connection with the administration of justice*"[377] as well as processing of personal data "*carried out in accordance with the legislation of the Russian Federation concerning defence, security, counter-terrorism, transport safety, anti-corruption measures, investigative activities and enforcement proceedings and the penal legislation of the Russian Federation*"[378]. The exceptions provide relatively large caveats.

Further, Chapter 3 of the Personal Data Law provides mechanisms to protect the rights of data subjects. These concern among others the right to access[379] and the right to appeal against actions (or inaction) of an operator[380]. These rights are accompanied by corresponding obligations for operators in Chapter 4. However, the rights of data subjects are almost always accompanied by the possibility that federal laws state otherwise, without specifying these laws. According to Article 22 of the Personal Data Law, the operator is obliged to notify the processing to the *Roskomnadzor* prior to conducting any type of processing, unless one of the listed exceptions apply. No notification is needed to the data subject.

iii. The Data Protection Act

It can be held that the Data Protection Act imposes also information rights applicable to operators. These rights are similar as the ones provided under the Personal Data Law. It also requires operators to publish a data processing policy.

[367] Article 5(4) of the Personal Data Law.
[368] Article 5(6) of the Personal Data Law.
[369] Article 5(7) of the Personal Data Law.
[370] Article 6 of the Personal Data Law.
[371] Article 6(1) of the Personal Data Law.
[372] Article 6(2) of the Personal Data Law.
[373] Article 6(3) of the Personal Data Law.
[374] Article 6(11) of the Personal Data Law.
[375] Article 10 of the Personal Data Law.
[376] Article 10(2) of the Personal Data Law.
[377] Article 10(6) of the Personal Data Law.
[378] Article 10(7) of the Personal Data Law.
[379] Article 14 of the Personal Data Law, in particular Paragraph 7.
[380] Article 17 of the Personal Data Law.

2.3.4 Upcoming changes in legislation

In 2020, the Russian lower parliamentary chamber (the Duma) adopted bill No. 759897-7, which sets up a federal database, comprising all personal data of all Russian citizens[381]. The database will contain personal data such as birth certificates, passport details, marital status, any change of gender, education, residence permits abroad, employment, and taxpayers' information. The database will also include references between parents' and children's' profiles. The database is expected to be up and running by 2025.

According to Human Rights Watch (HRW), the justification for the law is related to a need to ensure reliability and consistency of data across the country[382]. The concerns of the HRW are that "*the uniform database concept allows the government to store excessive amounts of data indefinitely as well as share it with governmental agencies without a person's explicit consent*"[383].

2.3.5 Intermediary conclusion

In relation to Russia, it can be concluded that Russian data protection law is a complex matter. Although the formal legislative framework seems comprehensive, the enforcement and the application of the legislation has serious drawbacks. In addition, Russia has a striking record of violating the ECHR related to other related rights and freedoms, such as the freedom of expression. Especially in relation to the interests of national security, the right to data protection and privacy is limited. This was also stated by the ECtHR in the *Roman Zakharov v. Russia* case. Considering the close correlation between the ECHR and the EU-Charter, careful consideration should be given to personal data transfers to Russia. Further, when it comes to state surveillance and data protection, some scholars argue, that digitalisation has led to new types of surveillance and possibilities of censorship and information controls. This reflects one of the major findings of this report - that authorities tend to use data protection laws as an instrument to enforce political aspirations, maintain control of the internet, and protect the interests of the government. Finally, compared to the EU, Russian authorities take a significantly more negative approach to balancing fundamental rights in the digital sphere, putting the protection of the State before the interests and rights of data subjects.

Laws/ Features	Scope of Government Access	Oversight	Remedy/Data Subjects' Rights
The Personal Data Law (Federal Law No. 152-FZ)	State agencies are thereby bound by the provisions of the Personal Data Law. No provisions directly related to Government Access.	Operators are obliged to notify the processing to *Roskomnadzor* prior to the processing (certain exceptions exist).	Processing limited to the achievement of specific, predetermined and legitimate goals; Purpose limitation; Removal/clarification incomplete or inaccurate data, and destruction or depersonalisation upon achievement of the processing goals;

[381] Bill No. 759897-7 On the Unified Federal Information Register containing information on the population of the Russian Federation, viewed 31 August 2021, https://sozd.duma.gov.ru/bill/759897-7, as described by HRW, "New Database Threatens Right to Privacy in Russia", viewed 31 August 2021, https://www.hrw.org/news/2020/05/26/new-database-threatens-right-privacy-russia.

[382] HRW referring to the documents from the legislative procedures, viewed 31 August 2021, https://sozd.duma.gov.ru/bill/759897-7.

[383] HRW, "New Database Threatens Right to Privacy in Russia", viewed 31 August 2021, https://www.hrw.org/news/2020/05/26/new-database-threatens-right-privacy-russia.

			Conditions of processing personal data (such as consent); Special provisions for the processing of biometric and special categories of personal data; The right to access; The right to appeal against actions (or inaction) of an operator + corresponding obligations or operators to ensure the rights.
Data Protection Act (Federal Law No. 149-FZ)	Obligation for internet operators to store text messages, voice communications, images, audio, video and other messages communicated by users located in Russia for six months. Messages and metadata of users should be stored for one year. Telecommunication providers are also required to store all internet traffic data for 30 days.	Requirement for controllers to notify *Roskomnadzor* prior to processing personal data.	N/A
Data Localisation Law (Federal Law No. 242-FZ)	Obligations for operators to make sure that recoding, systematisation, accumulation, storage, refining and retrieving of personal data is carried out for data bases located at Russian territory. This obligation targets both Russian companies storing data abroad, as well as foreign operators who are active in Russia. Operators must ensure that information on the physical localisation of the servers are available.	See Federal Law 149-FZ, as Data Localisation Law amends that.	N/A
Federal Law of March 6, 2006 No. 35-Fz on counter-terrorism - *Yarovaya* package	Obligation for telecom operators to store: ■ calls and messages (including pictures, videos and audio recordings) of subscribers for a period of up to six months; ■ 'information about subscribers' messages' for a period of up to three years and one year for Internet-based messenger services; ■ extensive information on users such as mobile phone number, IMSI, CDMA, login, IP address, email, PIN code, full name, national ID data.	N/A	The 2018 Resolution on Internet Traffic provides state intelligence and surveillance authorities with unmonitored access to the data accumulated based on abovementioned obligations.

	Obligation for internet-based messenger services operators to provide data on decoding users` messages to local divisions of the FSB.		
Bill No. 759897-7, (not yet in force)	Establishment of federal database, comprising all personal data of all Russian citizens.	N/A	Authorities will have access to the data *ex officio*.

3 CONCLUSION

The present study preliminarily investigates the general situation of China, India and Russia concerning fundamental rights and freedoms, in particular as regards the right to privacy and data protection. Secondly, the study contains an analysis of the legislation of the countries in order to establish the substantive and procedural conditions for government access to personal data, including law enforcement and intelligence agencies, with an attention to the authorities involved in the adoption or amendment of the related rules and decisions. Afterwards, the study investigates whether specific purposes and conditions to access personal data of foreign individuals exist in each of the three countries. The study also aims to identify, where existing, oversight mechanisms on the governmental access to personal data, and to assess the independency from the executive of the bodies empowered to perform such control. Finally, the study explains which rights and administrative or judicial redress mechanisms are available to data subjects (including foreign individuals) in the three observed countries.

In relation to China, it can be seen that the Chinese legal system does not provide sufficient safeguards for foreigners' data comparable to those found in the EU. Based on insights from the analysis of the People's Republic of China (PRC) Constitution it is clear that government access to personal data is not constrained. Especially the fact that its Constitution plainly states that the PRC is a dictatorship, where the power is concentrated in and executed by the Communist Party of China (CCP), makes this clear. Based on this, it can be argued that a legal environment for sufficient protection of personal data against government access does not exist - regardless of the normative content of the secondary laws. In relation to personal data, several secondary laws focused on national security and the public order provide for exemptions to privacy protection legislations. The notions of security and the public order are interpreted wider than in the EU and are considered priorities for the PRC's political system. The analysis of these secondary laws indicate that the government has leeway in accessing peoples' data. It can be concluded that Chinese law legitimises broad and unrestricted access to personal data by the government. Personal Information Protection Law (PIPL) and Data Security Law (DSL) could be seen as an effort to enhance data protection in PRC. However, they do not bring a substantial change to what the PRC government will be able to do with the peoples' data.

In relation to India, it should be noted that the right to privacy was recognised only recently by the Indian Supreme Court. In close connection, also the right to personal data has received more attention. However, the Indian government has a track record of infringing both rights extensively. After careful assessment of relevant Indian legislation (Information Technology Act - IT Act, several IT Rules and Aadhaar Act), it may be concluded that these regulations foresee widespread exemptions for governmental access to personal data. In general, the grounds justifying exceptional interception of data are broadly phrased and vague. More precisely, the concept of 'national security' is an umbrella concept used by the government to access personal information. Such information includes all data stored on the Indian territory. In other words, this can also involve personal data of people in the EU. In case of governmental access, it is true that several conditions need to be fulfilled. However, as mechanisms are not transparent there is little evidence that these conditions are fulfilled. In relation to data subjects' rights, it can be argued that this is rather limited. In relation to remedies it can be held that, only in a few cases is it possible for civilians to have access to a redress mechanism. In case of an infringement, the government itself remains mostly impenetrable. In the future, no additional protection for personal data seems to be upheld, as also the draft Personal Data Protection (PDP) Bill includes several exemptions for governmental agencies.

In relation to Russia, it can be concluded that Russian data protection law is a complex matter. Although the formal legislative framework seems comprehensive, the enforcement and the application of the legislation has serious drawbacks. In addition, Russia has a striking record of violating the European Convention of Human Rights (ECHR) related to other related rights and freedoms, such as the freedom of expression. Especially in relation to the interests of national security, the right to data protection and privacy is limited. This was also stated by the European Court of Human Rights (ECtHR) in the *Roman*

Zakharov v. Russia case. Considering the close correlation between the ECHR and the EU-Charter, careful consideration should be given to personal data transfers to Russia. Further, when it comes to state surveillance and data protection, some scholars argue, that digitalisation has led to new types of surveillance and possibilities of censorship and information controls. This reflects one of the major findings of this report, that authorities tend to use data protection laws as a means of enforcing political aspirations, maintaining control of the internet, and protecting the interests of the government. Finally, compared to the EU, Russian authorities take a significantly more negative approach to balancing fundamental rights in the digital sphere, putting protection of the State ahead of the interests and rights of data subjects.

ANNEX 1 – QUESTIONNAIRES

All interviewees received the same introduction and list of definitions. However, the actual questions were different, depending on the country and in the case of China, also on the background of the expert that was interviewed, as indicated below.

Introduction to the study

When transferring personal data to third countries outside the EU, data exporters and data importers have the responsibility to assess themselves that the legislation of the third country of destination enables the data importer to comply with any of the appropriate safeguards enshrined in Article 46 of the General Data Protection Regulation (GDPR). However, evaluating the legislation and practice in third countries on government access to data, especially concerning public security, defense and national security purposes, may be complex for controllers, processors, and even for data protection supervisory authorities, which play a key role to play when enforcing the GDPR and when issuing further decisions on transfers to third countries. To avoid divergent decisions, supervisory authorities will further work within the European Data Protection Board (EDPB) in order to ensure consistency, in particular if transfers to third countries must be prohibited.

Against that background, the EDPB has launched a study of which the goal is to collect objective, reliable and up-to-date background information on the legislation and practice in China on governments' access to personal data. Hence, the study must provide relevant information in order to facilitate this assessment mentioned in Article 46 of the GDPR. The following questionnaire is aimed at gathering information from data protection experts of three designated third countries, and accurately mapping the legal framework applicable to and relevant case law on governments' access to personal data.

The study is independent in its nature. Therefore, it does not represent the views of the EDPB or any individual supervisory authority and does not bind them in their assessment concerning data transfers.

Definitions

Personal data
This notion refers to any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person[384].

Government authorities
This notion should be understood broadly and shall encompass law enforcement authorities (e.g., police, public prosecutors, courts), government bodies, intelligence agencies …

Supervisory authority
This notion refers to an independent public authority which is responsible for monitoring the compliance with data protection and fundamental rights[385].

Law enforcement authority
This notion refers to

- *any public authority competent for the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security; and*

[384] Article 4 GDPR.
[385] Cf. Article 51 GDPR.

- *any other body or entity entrusted by Member State law to exercise public authority and public powers for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security*[386].

Access to data for law enforcement purposes
This notion shall be interpreted as broadly as possible, covering purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security and/or similar purposes[387].

Data subject rights
The notion refers to any right allowing data subjects to exercise a control over the processing of their personal data. According to the GDPR data subjects whose personal data is being processed, can exercise different rights, such as the right to access, the right to rectification, the right to erasure, the right to restriction of processing, and the right to object at any time to processing of personal data[388].

I. CHINA

Questions to legal practitioners

How does the government authorities' access (including law enforcement and intelligence authorities) to personal data in China look like from the perspective of legal practice?

1.1. Are there any official queries issued by the government authorities?
1.2. In what circumstances do private (including foreign companies) need to disclose the data to the government authorities?
1.3. In what way can government authorities obtain personal data in practice?
1.4. Is there any piece of evidence of the government authorities seeking access into the cyber systems, as well as to physical premises, to obtain data from foreign companies based in China?

Questions to legal practitioners and scholars

What is the case law of Chinese courts when claiming privacy rights against the government authorities, stipulated, e.g., in Civil Code and other laws?

1.1 Does there exist any legal doctrine or practice developed by courts?
1.2 To what extent it is possible to successfully claim one's rights concerning personal data? Is it encouraged or discouraged?

Questions to legal scholars

1. Under Article 40 of the Constitution and other laws regulating confidentiality of correspondence, there is a reference to the concept of the citizen rather than "everyone" or "individuals". How does the protection of citizens and foreigners differ with regard to the protection against access to personal data by government authorities?

[386] Article 3(7) of the Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA (LED), OJ L 119, 4.5.2016, p. 89-131, viewed 7 September 2021, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016L0680.
[387] Article 1 LED.
[388] Chapter III GDPR.

2. What safeguards are provided under Criminal Procedural Law for access to personal data by government authorities?

3. What are the remedies provided for individuals in case of violation of these rules?

4. Do foreigners residing inside or outside of China have the remedies in case of a breach of Criminal Procedural Law?

5. According to Article 26 of the Chinese National Intelligence Act, national intelligence institutions shall supervise and oversee the staff's compliance with laws and discipline. In addition, Article 27 of this Act states that national intelligence agencies must have certain outlets for input or complaints. However, it is unclear how these complaints are treated and what the nature of these complaints mechanisms is. Is there any redress mechanism provided for access by the government to the personal data of data subjects living outside China for intelligence activities?

6. To what extent can general administrative law remedies be applied to access to personal data by government authorities?
    8.1. If yes, can foreigners residing outside China invoke these remedies?
    8.2. How do those remedies work in practice?

II. INDIA[389]

Rule of law, respect of human rights and right to privacy in India

1. How is the general situation regarding rule of law, respect for human rights and fundamental freedoms, and in particular the right to privacy and data protection, perceived amongst legal practitioners and privacy advocates, also in light of the participation of India to the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights?
2. What is the impact of the judgment of the Supreme Court of India Justice K.S. Puttaswamy & another Vs. Union of India, delivered in August 2017 and recognizing the right to privacy as a fundamental right under Article 21 of the Constitution, on the general attitude of the Indian Courts toward privacy rights and their enforcement?
3. What role do Mutual Legal Assistance Treaties/Agreements on Criminal Matters (with the 39 countries) play in the criminal prosecution? Do these cooperation agreements have a strong practical impact for India law enforcement authorities?

Aadhaar Act 2019 – Aadhar and Other Laws (Amendment) Act 2019 – Telegraph Act, Prevention of Money Laundering Act

4. In your view, does the Aadhaar and Other Laws (Amendment) Act 2019 comply with the Supreme Court judgment Justice K.S. Puttaswamy & another Vs. Union of India?
5. *Section 27 of the Aadhaar and Other Laws (amendment) Act 2019, which amends the Prevention of Money-Laundering Act 2002, gives the Central Government the power to permit, by notification, a reporting entity other than a banking company to perform authentication under the Aadhar Act 2016, if it deems it necessary or expedient to do so.* How are the requirements of necessity and expediency substantiated in similar decisions of the Government?
6. What is the practical procedure leading to the permission of the Government as mentioned under Section 27?
7. Are the data subjects involved in such procedure at any stage: before, during or after the processing of their personal data linked to the Aadhaar number?

Information Technology Act 2000 (IT Act)

8. *Section 69 of the Information Technology Act 2000 provides that the Central Government or to a State Government, if satisfied that is necessary or expedient so to do, in the interest of the*

[389] All questions were asked to all experts. No distinction was made according to the capacity of the interviewee.

sovereignty of and integrity of India, defence of India, security of the State, friendly relations with foreign States or public order or for preventing incitement to the commission of any cognizable offence specified under the IT Act, or for investigation of any offence, may direct any Government agency to intercept, monitor or decrypt or cause to be intercepted or monitored or decrypted any information generated, transmitted, received or stored in any computer resource. What are the conditions under which the requirement of necessity or expediency is fulfilled?

9. Which institutions are involved in the decisional procedure about the fulfilment of such requirements?
10. Is a judicial warrant needed in order to direct the Government agencies to intercept, monitor or decrypt the information in question?
11. What is the practical procedure to issue such order of the Government?
12. How are the concepts of "sovereignty or integrity of India", "defence of India", "security of the State", "friendly relations with foreign States" or "public order" substantiated under Indian law?
13. What is the level of discretion left to the authorities in assessing whether similar grounds justify the interception, monitoring or decryption?
14. Does any relevant case law exist with regard to the interpretation of these conditions and legal grounds?
15. Do such provisions and conditions apply where personal data of foreign individuals are included in the information to be intercepted, monitored or decrypted?
16. *According to Section 69B, the Central Government may, to enhance cyber security and for identification, analysis and prevention of intrusion or spread of computer contaminant in the country, by notification in the Official Gazette, authorize any agency of the government to monitor and collect traffic data or information generated, transmitted, received or stored in any computer resource*. What is the procedure to be followed in order to issue the authorization and previous to the notification in the Official Gazette?
17. Do such provisions and conditions apply where personal data of non-Indian individuals are included in the traffic data or information?
18. Section 87 of the Act *gives the Central Government the power to make rules to carry out the provisions of the Act, in particular about the procedures and safeguards for interception, monitoring or decryption under Section 69; such rules shall be laid before each House of Parliament while it is in session so that it agrees before the expiry date of thirty days in making any modification or that the rules should not be made. In this case, the rule has effect in the modified form or is of no effect, as far as such modification or annulment is without prejudice to the validity of anything previously done under that rule.* Where the modification or annulment may cause a prejudice to the validity of anything previously done under the rule, does the Parliament retain the power to amend or reject the rule in question?
19. Are the Adjudicating Officer, as appointed by the Government under Section 46 of the IT Act, and the Appellate Tribunal, as identified under Section 48 of the IT Act, competent in adjudging any controversy arising from the processing of personal data according to Sections 69 and 69B of the IT Act?
20. How is the independency of the Adjudicating Officer and of the Appellate Tribunal guaranteed in this regard?
21. *According to Section 84 of the Information Technology Act 2000, no suit, prosecution or other legal proceeding shall lie against the Central Government, the State Government, the Controller or any person acting on behalf of him, and adjudicating officers for anything which is in good faith done or intended to be done in pursuance of this Act or any rule, regulation or order made thereunder.* How do Indian Courts substantiate the requirement of good faith?
22. Does the absence of good faith represent a circumstance of inadmissibility of the action in Court?

Personal Data Protection Act 2019 (PDPA 2019)

23. What is your general view as regards to the potential effectiveness and approximate timeline for adoption and implementation of the Personal Data Protection Act 2019?

24. In light of the exemptions provided under Section 35 of the PDPA 2019, will any residual oversight mechanism over the government access to personal data by administrative and/or judicial bodies be in place?
25. How is the power conferred to the Government under Section 86 of the PDPA 2019 to issue directions to the Data Protection Authority when the sovereignty and integrity of India, the security of the State, friendly relations with third countries or public order come at stake, is likely to impact the independency of the Data Protection Authority?
26. *Section 2 of the PDPA 2019 will extent the application of the Act to the processing of personal data when such processing is carried out in within the territory of India or by any legal or physical person incorporated or created under Indian law.* In your view, does the PDPA 2019 encompass any specific guarantees for the personal data of foreign individuals?
27. Why does the PDPA 2019, in your opinion, not encompass a right to object to the processing of personal data of a data subject, on grounds relating to his or her particular situation, similar to the one enshrined in Article 21 of the EU General Data Protection Regulation (GDPR)?

III. RUSSIA[390]

1. How is general access to personal data by government authorities regulated in Russia?
   1.1. Are there differences with regard to access to personal data for law enforcement purposes or national security/intelligence purposes?
   1.2. Is access to personal data for intelligence purposes subject to specific conditions?

2. How are potential access restrictions applied in practice for different purposes (law enforcement, national security and intelligence)?
   2.1. Do government authorities in general observe and evaluate the effects on the rights of individuals (data subjects) when assessing access requests?
   2.2. Are there means intended to protect the right to effective remedy?
   2.3. Do courts/supervisory bodies in general give precedence to the rights of individuals (data subjects) when interpreting and applying the data protection legislation?

3. Attention to data subjects' rights (right to access, right to information, rights regarding automated decision-making, right to appeal)
   3.1. How are data subjects' rights regarded and prioritised in general?
   3.2. Would you say that the means to practice and enforce data subjects' rights are efficient?
   3.3. Would you say that the data subjects have access to effective judicial protection (as defined by the Court of Justice of the European Union (CJEU), the European Court of Human Right (ECtHR), the Charter of Fundamental Rights of the European Union, and the European Convention on Human Rights?
   3.4. If the answer to Q 3.2 and 3.3 is "no" – why not?
   3.5. What is the role of the *Roskomnadszor* (IT, communications, and data protection agency) when it comes to the protection of data subjects' rights?
      3.5.1. In theory?
      3.5.2. In practice?

4. Practice of enforcing data subjects' rights
   4.1. Would you say that fines and other enforcement mechanisms for ensuring data protection are:
      4.1.1. objectively applied?
      4.1.2. consistently applied?
   4.2. On the approach of the supervisory authority (*Roskomnadszor*) and courts (local and supreme courts)

[390] All questions were asked to all experts. No distinction was made according to the capacity of the interviewee.

4.2.1. How would you consider that functions of *Roskmonadszor* can be compared to a Data Protection Authority (DPA) according to General Data Protection Regulation (GDPR) What is the role of the *Roskomnasdzor* in relation to data subjects' rights in practice?
4.2.2. Would you consider that the (supreme) courts apply the data protection legislation consistently?
4.2.3. Would you say, in general, that courts (local and supreme) give data subjects' protection a strong standing in their practice?

5. Attention to the rights of EU citizens?
   5.1. Does data protection legislation also apply to individuals with another nationality than the Russian one
      5.1.1. If they are in Russia?
      5.1.2. If the data is located outside of Russia, but processed by Russian authorities?

6. How does the Russian legislation treat the retention and access to personal data?
   6.1. Are there any discrepancies between the level of protection of data subjects' rights when it comes to processing metadata for private (commercial) purposes and for law enforcement and combating terrorism (According to the Law of Russian Federation N-35 ФЗ 'On combating terrorism')?
   6.2. Considering the potential sensitivity of communication data (as per the case law of the CJEU), do you consider communication data to enjoy the same level of protection as personal data, especially in the practice of authorities and national courts?
      6.2.1. Especially for law enforcement and intelligence purposes?
      6.2.2. Considering both retention of metadata AND access to that data?

ANNEX 2 – SOURCES OF INFORMATION

EU

I. REGULATION

Charter of Fundamental Rights of the European Union, OJ C 326, 26.10.2012, p. 391–40, viewed 6 September 2021, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:12012P/TXT.

Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32002L0058&from=EN.

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679.

Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA (LED), OJ L 119, 4.5.2016, p. 89-131, viewed 7 September 2021, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016L0680.

II. CASE LAW

CJEU 20 October 2020, C-623/27, *Privacy International.*
CJEU 6 October 2020, C-511/18, C-512/18 and C-520/18, *La Quadrature du Net.*
CJEU 2 March 2021, C-746/18, *Prokuratuur.*
CJEU 16 July 2020, C-311/18, *Schrems II*.
CJEU 21 December 2016, C-203/15 and C-698/15, *Tele2 Sverige.*
CJEU 6 October 2015, C-362/14, *Schrems I.*
CJEU 8 April 2014, C-293/12 and C-594/12, *Digital Rights.*
CJEU 26 July 2017, *Opinion 1/15 on the EU-Canada PNR Agreement.*

ECtHR 25 May 2021, *Big Brother Watch and Others/The United Kingdom*, No. 58170/13, 62322/14 and 24960/15.

III. DOCTRINE

Watt, E., "Much Ado About Mass Surveillance – the ECtHR Grand Chamber 'Opens the Gates of an Electronic "Big Brother" in Europe' in Big Brother Watch v UK", *Strasbourg Observers* viewed 28 June 2021, https://strasbourgobservers.com/.

Tracol, X. (2019). Ministerio fiscal: Access of public authorities to personal data retained by providers of electronic communications services. European Data Protection Law Review (EDPL), vol. 5(1), pp. 127-135.

IV. OTHER SOURCES

EDPB, *Guidelines 10/2020 on restrictions under Article 23 GDPR*, 15 December 2020.

EDPB, *Recommendations 02/2020 on the European Essential Guarantees for surveillance measures*, 10 November 2020.

EDPS, *Case Law Digest: Transfers of personal data to third countries*, 10 June 2021.

EDPS, *Guidelines on assessing the proportionality of measures that limit the fundamental rights to privacy and to the protection of personal data*, 19 December 2019.

China

I. REGULATIONS

Administrative Procedure Law of the PRC, viewed 19 August 2021, http://www.npc.gov.cn/zgrdw/englishnpc/Law/2007-12/12/content_1383912.htm.

Civil Code of the People's Republic of China, viewed 28 July 2021, http://english.www.gov.cn/archive/lawsregulations/202012/31/content_WS5fedad98c6d0f72576943005.html.

Constitution of the PRC 2017, http://english.www.gov.cn/archive/lawsregulations/201911/20/content_WS5ed8856ec6d0b3f0e9499913.html.

Counter-espionage Law of the PRC 2014, https://www.chinalawtranslate.com/en/anti-espionage/

Cybersecurity Law of the People's Republic of China 2017,https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-cybersecurity-law-peoples-republic-china/.

Data Security Law of the PRC 2021 (effective as of 1 September 2021), https://digichina.stanford.edu/news/translation-data-security-law-peoples-republic-china.

National Intelligence Law of the P.R.C. 2017, https://www.chinalawtranslate.com/national-intelligence-law-of-the-p-r-c-2017/?lang=en.

National Security Law of the PRC 2015, https://www.chinalawtranslate.com/en/2015nsl/#_Toc423592313.

Personal Information Protection Law of the PRC (Draft) (Second Review Draft) 2021, https://digichina.stanford.edu/news/translation-personal-information-protection-law-peoples-republic-china-draft-second-review.

State Compensation Law of the PRC, viewed 19 August 2021, http://www.china.org.cn/china/LegislationsForm2001-2010/2011-02/12/content_21905705.htm.

UN Treaty Body Database, https://tbinternet.ohchr.org/_layouts/15/TreatyBodyExternal/Treaty.aspx?CountryID=36&Lang=E.

II. DOCTRINE

a. Book Chapters

Wang, Z., 2017, 'Systematic Government Access to Private-Sector Data in China' in Fred C. and Dempsey, J. (ed), '*Bulk Collection: Systematic Government Access to Private-Sector Data*, Oxford University Press, pp. 241-258, p. 241, https://oxford.universitypressscholarship.com/view/10.1093/oso/9780190685515.001.0001/oso-9780190685515-chapter-11.

b. Journal Articles

Burnay, M., 2016, 'Bridging the EU-China's Gap on the Rule of Law?',Asia Europe Journal, vol. 14, no. 1, pp. 95–106, 101.

Castellucci, I., 2007, 'Rule of Law with Chinese Characteristics', Annual Survey of International & Comparative Law, vol. 1, no. 1, pp 35-92 http://digitalcommons.law.ggu.edu/annlsurvey/vol13/iss1/4.

Creemers, R., 2018, 'China's Social Credit System: An Evolving Practice of Control', viewed 21 July 2021., https://ssrn.com/abstract=3175792.

Geller, A., 2020, 'How Comprehensive Is Chinese Data Protection Law? A Systematisation of Chinese Data Protection Law from a European Perspective', GRUR International, Volume 69, Issue 12,

pp. 1191–1203, p. 1202, viewed 28 July 2021, https://academic.oup.com/grurint/article/69/12/1191/5909207.
Greenleaf, G., 2020, 'China issues a comprehensive draft data privacy law', Privacy Laws & Business International Report Vol. 168, No. 1, pp. 6-10, viewed 28 July 2021, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3795001.
LI, L., 2015, 'Rule of Law' in a Party-State: A Conceptual Interpretive Framework of the Constitutional Reality of China', 2 Asian Journal of Law and Society, 93. viewed 21 July 2021.
Li, T. and Bronfman, J. and Zhou, Z., 2017, 'Saving Face: Unfolding the Screen of Chinese Privacy Law' (August 2017). Journal of Law, Information, and Science (Forthcoming), pp. 1-33, p. 12 viewed 28 July 2021, https://ssrn.com/abstract=2826087.
Pernot-Leplay, E., 2020, 'China's Approach on Data Privacy Law: A Third Way Between the U.S. and the E.U.?, PENN. ST. J.L. & INT'L AFF., vol. 8, no. 1, pp. 49-117, viewed 28 July 2021, https://elibrary.law.psu.edu/cgi/viewcontent.cgi?article=1244&context=jlia.
Qi, A. and Guosong, S. and Wentong, Z., 2018, 'Assessing China's Cybersecurity Law', Computer Law & Security Review Volume 34, Issue 6, pp. 1342-1354, viewed 28 July 2021, https://www.sciencedirect.com/science/article/abs/pii/S0267364918303157.
Ruskola, T., 2003, 'Law without law, or is chinese law an oxymoron', William & Mary Bill of Rights Journal 11(2), pp. 655-670.
Von Blomberg, M., 2018, 'The Social Credit System And China's Rule Of Law', Mapping China Journal, pp.77-162, viewed 21 July 2021.
Yang, F. and Feng, J., 2021, 'Rules of electronic data in criminal cases in China', International Journal of Law, Crime and Justice, Vol. 64, pp. 1-11, https://www.sciencedirect.com/science/article/pii/S1756061620304882#:~:text=The%20amendment%20to%20the%20Criminal,physical%20evidence%20nor%20documentary%20evidence.
Zhizheng, W., 2012, 'Systematic government access to private-sector data in China, *International Data Privacy Law*, Volume 2, Issue 4, pp. 220–229, viewed 21th July 2021.

III. OTHER SOURCES

Amnesty International, Everything you need to know about human rights in China | Amnesty International | Amnesty International, viewed 13 September 2021, https://www.amnesty.org/en/countries/asia-and-the-pacific/china/report-china/.
Hoffman S. and Kania, E., 2018, 'Huawei and the ambiguity of China's intelligence and counter-espionage laws', viewed 28 July 2021, https://www.aspistrategist.org.au/huawei-and-the-ambiguity-of-chinas-intelligence-and-counter-espionage-laws/.
Hoffman, S. and Attrill, N., 2021, 'Mapping China's Technology Giants: Supply chains and the global data collection ecosystem', viewed 28 July 2021, https://www.aspi.org.au/report/mapping-chinas-tech-giants-supply-chains-and-global-data-collection-ecosystem.
Hoffman, S., 2019, 'Engineering global consent: The Chinese Communist Party's data-driven power expansion', https://www.aspi.org.au/report/engineering-global-consent-chinese-communist-partys-data-driven-power-expansion.
Horsley, J. P., 2021, 'How will China's privacy law apply to the Chinese state?', viewed 28 July 2021, https://www.newamerica.org/cybersecurity-initiative/digichina/blog/how-will-chinas-privacy-law-apply-to-the-chinese-state/.
Huawei, 2021, Huawei Facts, https://www.huawei.com/uk/facts/question-answer/hw-cooperate-with-chinas-intelligence-community-how-can-we-trust-you.
Human Rights Watch, 2019, China's Algorithms of Repression Reverse Engineering a Xinjiang Police Mass Surveillance App, viewed 28 July 2021, https://www.hrw.org/report/2019/05/01/chinas-algorithms-repression/reverse-engineering-xinjiang-police-mass.
Human Rights Watch, Detention and Torture in the Chinese Communist Party's Shuanggui System | HRW, viewed 8 August 2021 https://www.hrw.org/report/2016/12/06/special-measures/detention-and-torture-chinese-communist-partys-shuanggui-system.

Ji, H. and Fang, J., 2017, 'Costs and unanswered questions of China's new cybersecurity regime', viewed 28 July 2021, https://iapp.org/news/a/costs-and-unanswered-questions-of-chinas-new-cybersecurity-regime/.
Kenyon, M., 'Christopher Parsons Delivers Testimony to Special Committee on Canada-China Relations' viewed 28 July 2021, https://citizenlab.ca/2021/03/christopher-parsons-delivers-testimony-to-special-committee-on-canada-china-relations/.
Lin, P., 2021, 'Tiktok v. Douyin A Security and Privacy Analysis, https://citizenlab.ca/2021/03/tiktok-vs-douyin-security-privacy-analysis/.
Laskai L. and Segal A., 2021, 'The Encryption Debate in China: 2021 Update', viewed 14 October 2021, https://carnegieendowment.org/2021/03/31/encryption-debate-in-china-2021-update-pub-84218.
Mannheimer Swartling, 2019, 'Applicability of Chinese National Intelligence Law to Chinese and non-Chinese Entities', viewed 28 July 2021, https://www.mannheimerswartling.se/app/uploads/2021/04/msa_nyhetsbrev_national-intelligence-law_jan-19.pdf.
Moritz, R., 2021, 'Xi Jinping Thought on the Rule of Law, https://www.swp-berlin.org/publications/products/comments/2021C28_Jinping_RuleOfLaw.pdf.
NPC Observer, https://npcobserver.com/legislation/personal-information-protection-law/.
Susan, N. and others, 2021, 'China Data Protection Paths under Data Security Law' viewed 28 July 2021, https://www.chinalawinsight.com/2021/06/articles/uncategorized/china-data-protection-paths-under-data-security-law/#_ftn3.
Tanner, M. S., 2017, 'Beijing's New National Intelligence Law: From Defense to Offense', viewed 28 July 2021 https://www.lawfareblog.com/beijings-new-national-intelligence-law-defense-offense.

INDIA

I. REGULATIONS

Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016, https://uidai.gov.in/images/targeted_delivery_of_financial_and_other_subsidies_benefits_and_services_13072016.pdf.
Constitution of India, https://legislative.gov.in/Constitution-of-india.
Information Technology Act 2000, https://legislative.gov.in/sites/default/files/A2000-21_0.pdf.
Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules 2021, https://www.meity.gov.in/writereaddata/files/Intermediary_Guidelines_and_Digital_Media_Ethics_Code_Rules-2021.pdf.
Information Technology (Procedures and Safeguards for Interception, Monitoring and Decryption of Information) Rules 2009, https://cis-india.org/internet-governance/resources/it-procedure-and-safeguards-for-interception-monitoring-and-decryption-of-information-rules-2009.
Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011, https://www.wipo.int/edocs/lexdocs/laws/en/in/in098en.pdf.
Indian Personal Data Protection Bill [Draft], 2019, http://164.100.47.4/BillsTexts/LSBillTexts/Asintroduced/373_2019_LS_Eng.pdf.
International Covenant on Civil and Political Rights, United nations, 1966, https://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx.
Universal Declaration of Human Rights, United nations, 1948, https://www.un.org/sites/un2.un.org/files/udhr.pdf.

II. CASE LAW

Supreme Court of India, 24 August 2017, WP(C) 494/2012, Justice K. S. Puttaswamy v. Union of India, https://scobserver-

production.s3.amazonaws.com/uploads/case_document/document_upload/624/Right_to_Privacy__Puttaswamy_Judgment_.pdf.
Indian Supreme Court, Puttaswamy v. Union of India, 26 September 2018, https://indiankanoon.org/doc/127517806/?__cf_chl_jschl_tk__=pmd_a67c88aecbdd553037db84bf6874a35053cbe28e-1629107044-0-gqNtZGzNAiKjcnBszQi6.

III. DOCTRINE

a. Book Chapters

Baxi, U. "The Colonialist Heritage" in Pierre Legrand and Roderick Munday (eds.), Comparative Legal Studies: Traditions and Transitions, Cambridge University Press, 2003.

b. Journal Articles

Bhandari V. and Sane R. (2019). A Critique of the Aadhaar Legal Framework. National Law School of India Review, 31(1), 72-97.
Bhandari, V. Sane R. (2018). Protecting Citizens from the State Post Puttaswamy: Analysing the Privacy Implications of the Justice Srikrishna Committee Report and the Data Protection Bill. Socio-Legal Review, 14(2), 143-169.
Chhugani, S., 2021, India's aadhaar card a violation of Indian citizen's right to privacy, Cardozo International & Comparative Law Review, vol. 4(2), pp. 733-762.
Deva Prasad, M. and Suchita Menon, C., 2020, The Personal Data Protection Bill, 2018: India's regulatory journey towards a comprehensive data protection law, International Journal of Law and Information Technology, pp. 1-19.
Rajesh Bahuguna, R., 2020, Relevance of Distinction between Sovreign and Non-Sovereign Functions in governmental Liability In the Field of Cyber Torts: Indian Perspective, Journal of Critical Reviews, vol. 7, issue 14, pp. 4226-4230, http://www.jcreview.com/fulltext/197-1599744495.pdf.
Rubinstein, I.S., Nojeim, G. T, Lee, R.D., 2014, Systematic government access to personal data: a comparative analysis, International Data Privacy Law, vol. 4(2), pp. 96–119, https://doi.org/10.1093/idpl/ipu004.

IV. REPORTS

Centre for Internet and Society. (20 February 2020). An Annotated Version of the Personal Data Protection Bill 2019, annotated-ver-pdp-bill-2019 (cis-india.org).
Committee of Experts under the Chairmanship of Justice B.N. Srikrishna, "A free and fair digital economy. Protecting Privacy, empowering Indians", https://www.meity.gov.in/writereaddata/files/Data_Protection_Committee_Report.pdf.
HRW. (7 June 2013). India: New Monitoring System Threatens Rights [Blog Post], viewed on 3 June 2021, retrieved from: https://www.hrw.org/news/2013/06/07/india-new-monitoring-system-threatens-rights.
HRW. (2020). Indian Events of 2020, viewed 3 June 2021, https://www.hrw.org/world-report/2021/country-chapters/india.

V. OTHER SOURCES

Chowdhury P., Thayil K. (25 January 2021). Data Privacy in India [Blog post] Retrieved from https://www.mondaq.com/india/privacy/1005640/data-privacy-comparative-guide.
Digital India Programme, https://www.digitalindia.gov.in/.
National human rights commission, India, https://nhrc.nic.in/acts-&-rules/declarationcovenants-1.
National Portal India, https://www.india.gov.in/my-government.
Order of the Ministry of Home Affairs (Cyber and Information Security Division) of the 20 December 2018, https://egazette.nic.in/WriteReadData/2018/194066.pdf.

Ratification of International Human Rights Treaties-India, http://hrlibrary.umn.edu/research/ratification-india.html.
Save our Privacy. (27 July 2018). Initial statement on justice Srikrishna committee report, [Blog post] Retrieved from Save Our Privacy | Initial statement on Justice Srikrishna Committee.
Software Freedom Law Center. (1 August 2019). What has been changed in the Aadhaar Amendment Bill?. [Blog Post], Retrieved from https://sflc.in/what-has-been-changed-aadhaar-amendment-bill.
UN General Assembly, Human Rights Council, National report submitted in accordance with paragraph 5 of the annex to Human Rights Council resolution 16/21* India, February 2017. https://documents-dds-ny.un.org/doc/UNDOC/GEN/G17/044/56/PDF/G1704456.pdf?OpenElement.
UN General Assembly, Human Rights Council, Summary of Stakeholders' submissions on India, February 2017, https://documents-dds-ny.un.org/doc/UNDOC/GEN/G17/046/29/PDF/G1704629.pdf?OpenElement.
X. (1 December 2017). 1.3 Billion People's Right To Privacy Upheld Following Historic Judgement By India's Supreme Court', [Blog post]. Retrieved from https://privacyinternational.org/blog/768/13-billion-peoples-right-privacy-upheld-following-historic-judgement-indias-supreme-court.
X. (18 June 2020). India: RBI publishes framework on payment system operators, [Blog post] Retrieved from https://www.dataguidance.com/news/india-rbi-publishes-framework-payment-system-operators.

Russia

I. REGULATIONS

Constitution of the Russian Federation of 25 December 1993 with amendments.
Federal Law of 12.12.2015 N 7-FKK.
Federal Law of 27 July 2006 N 152-FZ on personal data, accessed 14.9.2021, https://pd.rkn.gov.ru/authority/p146/p164/.
Federal Law No. 149-FZ of July 27,2006 on information, information technologies and information protection, https://398-fz.rkn.gov.ru/docs/149-FZ.pdf (in Russian).
Federal Law of 06.07.2016 N 374-FZ.
Federal Law of 21.07.2014 N 242-FZ.
Federal Law of 31.12.2020 N 481-FZ.
Directive of the Bank of Russia No. 3889-U.
Order of the Federal Security Service No. 378.
Order of Ministry of Digital Development, Communications and Mass Media of the Russian Federation dated 29.10.2018 N 573.

II. CASE LAW

Constitutional Court of Russia, Judgement No. 12-П/2016.
ECtHR4 December 2015, Roman Zakharov v. Russia, No. 47143/06.
ECtHR 4 July 2013, Anchugov and Gladkov v Russia, App no 11157/04 and 15162/05.
ECtHR, Shimovolos v. Russia, App. No. 30194/09.
ECtHR, Vladimir Kharitonov v. Russia, App. No. 10795/14.

III. DOCTRINE

Aksenova, Marina and Iryna Marchuk, "Reinventing or Rediscovering International Law? The Russian Constitutional Court's Uneasy Dialogue with the European Court of Human Rights," Int J Const Law 16, no. 4 (31 December 2018).

Antonov, Mikhail, "Philosophy behind Human Rights: Valery Zorkin vs. the West?," in *Russia and the European Court of Human Rights*, ed. Mälksoo, Lauri and Wolfgang Benedek, 1st ed. (Cambridge University Press, 2017).

Bartenev, Dmitri, "LGBT Rights in Russia and European Human Rights Standards," in *Russia and the European Court of Human Rights: The Strasbourg Effect*, ed. Mälksoo, Lauri and Wolfgang Benedek, European Inter-University Centre for Human Rights and Democratisation (Cambridge: Cambridge University Press, 2017).

Gurkov, Alexander, "Personal Data Protection in Russia," in *The Palgrave Handbook of Digital Russia Studies*, ed. Gritsenko, Daria, Mariëlle Wijermars, and Mikhail Kopotev (Cham: Springer International Publishing, 2021).

Kalinichenko, Paul and Dimitry Vladimirovich Kochenov, "Amendments to the 1993 Constitution of the Russian Federation Concerning International Law (2020)," *International Legal Materials* 60, no. 2 (April 2021).

Moyakine, E. and A. Tabachnik, "Struggling to Strike the Right Balance between Interests at Stake: The 'Yarovaya', 'Fake News' and 'Disrespect' Laws as Examples of Ill-Conceived Legislation in the Age of Modern Technology," *Computer Law & Security Review* 40 (1 April 2021).

Muravyeva, Marianna and Alexander Gurkov, "Law and Digitization in Russia," in *The Palgrave Handbook of Digital Russia Studies*, ed. Gritsenko, Daria, Mariëlle Wijermars, and Mikhail Kopotev (Cham: Springer International Publishing, 2021).

Zhuravlev, Mikhail S. and Tatiana A. Brazhnik, "Russian Data Retention Requirements: Obligation to Store the Content of Communications," *Computer Law & Security Review* 34, no. 3 (1 June 2018).

IV. REPORTS

Amnesty International - Annual report 2020: https://www.amnesty.org/en/countries/europe-and-central-asia/russian-federation/report-russian-federation/.

UN Human Rights Committee, Concluding observations on the seveth periodic report of the Russian Federation, CCPR/C/RUS/CO/7, accessed 15.6.2021 via https://tbinternet.ohchr.org/_layouts/15/treatybodyexternal/Download.aspx?symbolno=CCPR/C/RUS/CO/7&Lang=En.

Human Rights House Foundation: "Russia: Telegram block leads to widespread assault on freedom of expression online", accessed 21.6.2021 via https://humanrightshouse.org/letters-of-concern/russia-telegram-block-leads-widespread-assault-freedom-expression-online/.

Human Rights Watch 2021 World Report on Russia, accessed 19.5.2021 via https://www.hrw.org/world-report/2021/country-chapters/russia.

Human Rights Watch "Russia Closing Down Media Freedoms", published 29 April 2021, accessed 21.6.2021 via https://www.hrw.org/news/2021/04/29/russia-closing-down-media-freedoms.

Human Rights House "Human Rights Council Members must strongly denounce Russia's domestic human rights violations", 10 February 2021, accessed 21 June 2021, https://humanrightshouse.org/statements/human-rights-council-members-must-strongly-denounce-russias-domestic-human-rights-violations/.

ANNEX 3 - ACRONYMS AND ABBREVIATIONS

I. GENERAL

Acronyms and Abbreviations	Meaning
CJEU	Court of Justice of the European Union
CoE	Council of Europe
Convention 108	Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data
Convention 108+	Convention 108+ on protection of individuals with regard to the Processing of Personal Data
EDPB	European Data Protection Board
EDPS	European Data Protection Supervisor
EEA	European Economic Area
ECHR	European Convention on Human Rights
ECtHR	European Court of Human Rights
EDPB	European Data Protection Board
EU	European Union
EU-Charter	Charter of Fundamental Rights of the European Union
GDPR	General Data Protection Regulation
HRC	United Nations Human Rights Council
ICCPR	International Covenant on Civil and Political Rights
SA(s)	Supervisory authority(-ies)
UDHR	Universal Declaration of Human Rights
UN	United Nations

II. CHINA

Acronyms and Abbreviations	Meaning
CCP	Chinese Communist Party
CSL	Cybersecurity Law
DSL	Data Security Law
NPC	National People's Congress
PIPL	Personal Information Protection Law
PRC	The People's Republic of China

III. INDIA

Acronyms and Abbreviations	Meaning
Aadhaar Card	Aadhaar Unique Identification Number
CMS	Centralized Monitoring System
IT Act	Information Technology Act
PDP Bill	Personal Data Protection Bill
Rules 2009	Information technology procedures and safeguards for interception, monitoring and decryption of information rules
Rules 2011	Reasonable security practices and procedures and sensitive personal data or information rules
Rules 2021	Information technology intermediary guidelines and digital media ethics code rules
UIDAI	Unique Identification Authority of India
UPR	Universal Periodic Review

IV. RUSSIA

Acronyms and Abbreviations	Meaning
CC	Constitutional Court
Data Protection Act	Federal Law No. 149-FZ on Information, information technologies and data protection
FSB	Federal Security Service of Russian Federation
OSAA	Operational Search Activities Act
HRW	Human Rights Watch
Personal Data Law	Federal Law No. 152-FZ