ARTICLE 19

Iran: Personal Data Protection and Safeguarding Draft Act

June 2019

Legal analysis

Executive Summary

The Government of Iran's proposals to protect the privacy rights of its citizens in the face of new threats brought by modern technologies, by introducing the Personal Data Protection and Safeguarding Draft Act, are a welcome effort. Overall, however, the Draft Act is poorly drafted and inconsistent with the international legal obligations of Iran to adequately protect the privacy rights of its citizens. The Draft Act departs from international standards on data protection and threatens the right to freedom of expression. ARTICLE 19 is also deeply concerned about the independence of the body in charge of overseeing the application of the Draft Act, as well as the lack of adequate remedies for individuals to counter violations of their rights and to seek compensation for any damage suffered. We urge the Iranian government to amend the Draft Act in accordance with the below recommendations, to ensure it complies with international human rights standards and properly protects the privacy rights of people in Iran.

Recommendations:

1. The Draft Act should be redrafted to reorganise and streamline, fully incorporating the principles set out in international law in the text of the law and in a specific section placed after Section Two that presents the "Definitions".

2. The Draft Act should include a specific provision regulating its material and territorial scope of application. The provision should clearly state that it will apply to all government entities as well as to private bodies. Currently, these rights are not adequately protected by other Iranian legislation. These changes should also be harmonised with the Publication and Free Access to Information Act of 2009.

3. Article 3 should be redrafted to bring it into line with the principle of non-discrimination, ensuring that the Bill applies to every individual - not just citizens and foreign citizens whose data are processed in the territory of Iran. In its current formulation, differentiating citizens and foreign citizens, as well as the exclusion of stateless citizens, the Draft Act violates Iran's international human rights obligations.

4. The Draft Act should specifically remove the application of privacy protections to corporations.

5. The Introduction should be redrafted in order to recall the right to freedom of expression as enshrined in the Constitution and to mention the Charter of Citizens' Rights that provides a framework for the protection of the right to freedom of expression, the right of access to information, the right to privacy, and to data protection in Iran. The Draft Act should take into account Iran's responsibilities as State party to the ICCPR, most notably Articles 17 (the right to privacy) and 19 (the right to freedom of expression).

6. Article 12 should be revised in order to include an exemption to processing that is intended to communicate information to the public, ideas, or opinions of general interest—including for journalistic purposes and the purposes of academic, artistic, or literary expression. Article 12 should also include assurances that due process is followed when accessing data without consent by better clarifying what the purpose of preventing or answering threats to order, security, or public safety means. Such terms could also be defined in Article 2 which presents "Definitions" in order not to empower authorities to abuse the rights of individuals, especially in efforts to repress and prosecute human rights defenders, minorities, journalists, bloggers, and activists.

7. The Draft Act should also ensure that journalists and other public interest communicators—including non-governmental organisations that are publishing information of public interest—are protected from being forced to reveal the sources of their information.

8. Ensure that any rules on the deletion of public information are balanced with freedom of expression and the public interest in accessing information and historical archiving by applying ARTICLE 19's seven-part test to the "right to be forgotten" in Article 9.

9. Remove requirements that all personal data be subject to data localisation.

10. Amend Article 12 to include an explicit exemption for personal information relating to public activities of public officials or others acting under public authority or spending public money to reflect the right of information enshrined in the Constitution and the public interest in obtaining information.

11. The Draft Act should specifically recognise the public interest provisions granted by the Publication and Free Access to Information Act to public bodies and ensure that the public interest is considered in any request.

12. Clarify Article 10 to ensure that persons have full and free access to their personal information held by third parties except in limited instances allowed under international law, most notably ICCPR General Comment No 16. Define what "public classified information" means under Article 10.

13. Grant data subjects a right of correction.

14. Ensure that the Commission is fully independent from the government and give it binding powers to order stopping of processing, correction, release of personal information to the subject, and other powers.

15. Give individuals a specific right to appeal the Commission's decisions to a court.

Table of Contents

About the ARTICLE 19 Transparency and MENA Programme

The ARTICLE 19 Transparency Programme advocates for the development of progressive standards on access to information at the international and regional levels, and their implementation in domestic legal systems. The Transparency Programme has produced a number of standard-setting publications, which outline international and comparative law and best practice in areas such as national security and privacy.

On the basis of these publications and ARTICLE 19's overall legal expertise, the Transparency Programme publishes a number of legal analyses, guides, and other materials each year, commenting on legislative proposals, as well as existing laws that affect the right to information, whistleblowing, data protection, and related rights. This analytical work frequently leads to substantial improvements in proposed or existing domestic legislation. All of our materials are available online at http://www.article19.org/

If you would like to discuss this analysis further, please contact David Banisar, Senior Legal Counsel and Head of Transparency of ARTICLE 19 at Banisar@article19.org.

The ARTICLE 19 Middle East and North Africa (MENA) programme focusses on a number of countries in the region with concerns over their records on freedom of expression in the world. Many countries in the region lack legal protections for human rights and the rule of law is undermined by a lack of independent judiciaries. The 2011 Arab Spring popular protests brought hope for improvements but devastating wars, foreign intervention, and instability have since made it an extremely dangerous environment for journalists, civil society, and human rights defenders, forcing millions to leave in search of safety. As war and conflict tear apart infrastructure and cause huge regression in development indicators across Yemen, Syria, Libya, and Iraq, elsewhere repressive governments in Saudi Arabia, Iran, Egypt, and Bahrain have reinforced anti-human rights practices, often in the name of national security and counterterrorism.

ARTICLE 19's work on Iran focuses on monitoring laws, policies, and regulations that affect freedom of expression and information online and offline. We monitor Iran's complex internet policies and respond to evolving threats online. We work with a wide network of experts and human rights defenders on how to effectively use Iran's freedom of information law and to highlight violations on freedom of expression and access to information.

If you would like to discuss the context and analysis of this Draft Act further, please contact Mahsa Alimardani at mahsa@article19.org.

I. Introduction

The right to privacy and the rights of freedom of expression and freedom of information are co-equal human rights. ARTICLE 19 believes they are complimentary rights which together empower citizens to protect their rights and to improve the transparency and accountability of public and private bodies that hold and wield power in society. ARTICLE 19 supports the adoption of well-designed data protection acts that protect individuals' rights while ensuring government transparency and freedom of expression.

In this analysis, ARTICLE 19 sets out its concerns regarding the Personal Data Protection and Safeguarding Draft Act (Draft Act) currently under discussion in the Iranian Parliament. The analysis explores its compatibility with Iran's international obligations under international human rights law to protect freedom of expression and information, as well as the right to privacy. The analysis then details the domestic legal framework. Ultimately, it reviews Draft Act's compliance with international law and makes recommendations to bring it in line with international and regional standards on freedom of expression and privacy.

II. Data Protection and Freedom of Expression and Information

A. The Right to Privacy

The right to privacy is considered essential in protecting an individual's ability to develop ideas and personal relationships. It is recognised in international human rights treaties including the Universal Declaration of Human Rights,[1] the International Covenant on Civil and Political Rights (ICCPR)[2], the European Convention on Human Rights,[3] the American Declaration of the Rights and Duties of Man,[4] and the American Convention on Human Rights.[5]

Under these treaties, privacy is a broad concept relating to the protection of individual autonomy and the relationship between an individual and society, including governments, companies, and other individuals. It is commonly recognised as a core right that underpins human dignity and other values. It is also understood as an enabler of the enjoyment and exercise of human rights online and offline, ranging from freedom of expression[6] and freedom of association and assembly, to the prohibition of discrimination.

At the regional level, the right to privacy is mostly recognised by non-binding legal instruments such as, most notably, the Cairo Declaration on Human Rights in Islam.[7] Article 18(b) states:

[1] UDHR, Art 12.

[2] ICCPR, Art 17.

[3] Art 8.

[4] Articles 5, 9, and 10.

[5] Art 11.

[6] Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression Frank La Rue, HRC 23/40, 17 April 2013 https://undocs.org/A/HRC/23/40 ; Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression David Kaye, HRC/29/32, 22 May 2015 https://undocs.org/A/HRC/29/32.

[7] Cairo Declaration on Human Rights in Islam, Aug. 5, 1990, U.N. GAOR, World Conf. on Hum. Rts., 4th Sess., Agenda Item 5, U.N. Doc. A/CONF.157/PC/62/Add.18 (1993) Art. 18 http://hrlibrary.umn.edu/instree/cairodeclaration.html.

> (b) Everyone shall have the right to privacy in the conduct of his private affairs, in his home, among his family, with regard to his property and his relationships. It is not permitted to spy on him, to place him under surveillance or to besmirch his good name. The State shall protect him from arbitrary interference.

1. Data Protection

The right to data protection is closely related to the right to privacy. It regulates the way in which information about individuals is collected, processed, stored and retained electronically by both public and private bodies. It has been recognised as both part of international law on privacy and has its own identity being acknowledged as autonomous right.

The UN Human Rights Committee has found that data protection is a fundamental part of privacy as protected by Article 17 of the ICCPR. The Committee in General Comment 16 stated that:

> The gathering and holding of personal information on computers, databanks and other devices, whether by public authorities or private individuals or bodies, must be regulated by law. Effective measures have to be taken by States to ensure that information concerning a person's private life does not reach the hands of persons who are not authorised by law to receive, process and use it, and is never used for purposes incompatible with the Covenant. In order to have the most effective protection of his private life, every individual should have the right to ascertain in an intelligible form, whether, and if so, what personal data is stored in automatic data files, and for what purposes. Every individual should also be able to ascertain which public authorities or private individuals or bodies control or may control their files. If such files contain incorrect personal data or have been collected or processed contrary to the provisions of the law, every individual should have the right to request rectification or elimination.[8]

Under international law, a number of basic principles have emerged:

- Information about persons should not be collected or processed in unfair and unlawful ways (principle of lawfulness and fairness). This includes obtaining information in an illegal manner such as illegal interceptions, unlawful access to databases and impersonations.

- Those responsible for the collection and processing must ensure it is accurate and, where necessary, kept up-to-date (to avoid error of omissions); every reasonable step must be taken to ensure that personal data which is inaccurate, having regard to the purposes for which it is processed, is erased or rectified without delay (principle of accuracy).

- Personal data shall be collected to serve a specific and legitimate purpose and shall be brought to the knowledge of the data subject (principle of purpose specification). Following application of this principle, data controllers and processors shall ensure that all personal data collected and recorded remain relevant and adequate to the purpose specified and are not used and disclosed for purposes incompatible with those specified and the period for which they are collected does not exceed that which would enable the achievement of the purposes so specified.

- Every data subject has the right to know whether information concerning him/her is being processed and to obtain it in an intelligible form, without undue delay or expense, and to have appropriate rectifications (principle of interested-person access).

- The prohibition of the collection of data that gives rise to unlawful and arbitrary discrimination, including information about racial or ethnic origin, colour, sex life, political opinions, religious, philosophical and other beliefs as well as membership of an association or trade union.

[8] *UN Human Rights Committee, General Comment No. 16: The right to respect of privacy, family, home and correspondence, and protection of honour and reputation (Art. 17) : 04/08/1988.*

- Finally, the principle of security states that reasonable and appropriate technical and organisational safeguards are in place to prevent unauthorised disclosure or breach of data.

These principles were adopted by the UN General Assembly in 1990 in a Resolution on guidelines for the data protection of personal information held in computer databases.[9] The Guidelines set out 6 basic principles of data protection based on fair information practices, namely the principles of lawfulness and fairness, accuracy, purpose specification, interested-person access, non-discrimination and security.

The right of privacy has also been further elaborated by the appointment by the UN Human Rights Council of a Special Rapporteur on the right to privacy[10] in the summer of 2015, and the adoption on 18 December 2013,[11] 21 January 2014,[12] and 19 December 2016[13] by the UN General Assembly and by the Human Rights Council on 22 March 2017[14] of resolutions on "the right to privacy in the digital age" as well as the recent Report of the United Nations High Commissioner for Human Rights.[15] The General Assembly in the latter resolution noted that "the increasing capabilities of business enterprises to collect, process and use personal data can pose a risk to the enjoyment of the right to privacy in the digital age" and called States to: "To develop or maintain and implement adequate legislation, with effective sanctions and remedies, that protects individuals against violations and abuses of the right to privacy, namely through the unlawful and arbitrary collection, processing, retention or use of personal data by individuals, governments, business enterprises and private organisations".[16]

2. Data Protection in Europe and Elsewhere

Europe is the only region where there is an explicit binding provision enshrining the right to data protection at a regional level, found in in the Charter of the Fundamental Rights of the European Union (CFREU).[17] The CFREU has acquired the same "constitutional" level as the founding treaties since the entry into force of the Treaty of Lisbon in 2009.[18] Article 8 of the CFREU not only affirms the right to personal data protection, but also spells out the core values associated with this right. It provides that the processing of personal data must be fair, for specified purposes, and based on either the consent of the person concerned or a legitimate basis laid down by law. Individuals must have the right to access their personal data and to have it rectified, and compliance with this right must be subject to control by an independent authority.

The EU General Data Protection Regulation (GDPR)[19] further specifies that the consent of the data subject shall be free, specific, informed, and unambiguous as a condition for lawful processing. It emphasises the principle of data minimisation

[9] Guidelines for the Regulation of Computerized Personal Data Files, G.A. res. 45/95, 14 December 1990, http://www.un.org/documents/ga/res/45/a45r095.htm.

[10] See OHCHR website, Special Rapporteur on the right to privacy: https://www.ohchr.org/en/issues/privacy/sr/pages/srprivacyindex.aspx.

[11] The right to privacy in the digital age, G.A. res. 68/167, 18 December 2013, http://www.un.org/ga/search/view_doc.asp?symbol=A/RES/68/167.

[12] The right to privacy in the digital age, G.A. res. 27/37, 21 January 2014, https://www.ohchr.org/documents/issues/digitalage/a-hrc-27-37_en.doc.

[13] The right to privacy in the digital age, G.A. res. 71/199, 19 December 2016, https://www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/71/199.

[14] The right to privacy in the digital age, HRC res. 34/L.7, 22 March 2017, https://documents-dds-ny.un.org/doc/UNDOC/LTD/G17/073/06/PDF/G1707306.pdf?OpenElement.

[15] The right to privacy in the digital age, Report of the United Nations High Commissioner for Human Rights, HRC res. 39/29, 3 August 2018, https://documents-dds-ny.un.org/doc/UNDOC/GEN/G18/239/58/PDF/G1823958.pdf?OpenElement.

[16] The right to privacy in the digital age, G.A. res. 71/199, 19 December 2016.

[17] European Union, Charter of Fundamental Rights of the European Union, 26 October 2012, 2012/C 326/02, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:12012P/TXT.

[18] Charter of Fundamental Rights of the European Union, Art. 8.

[19] 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&from=EN.

stipulating that personal data shall be adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed. [20]

The Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (usually known as the CoE Convention No. 108)[21] was adopted in 1981 and a "modernised" version was adopted by the Committee of Ministers on 18 May 2018. Convention 108 is the only legally binding international instrument in the data protection field with a worldwide scope of application. It is open for signature to member and non-member States of the Council of Europe (CoE) anywhere in the world.[22] To date, 55 countries are parties to Convention 108. They include all CoE member states (47 countries); Uruguay, the first non-European country to accede in August 2013; and Mauritius, Senegal, and Tunisia, which acceded in 2016 and 2017.

Data protection rights have also been adopted in administrative and legal procedures across the globe by the African Union, Organization of American States, OECD, Asia Pacific Economic Cooperation, and other international human rights, trade, and standards bodies.[23]

3. National Developments

These international developments have been strongly followed at the national level. As of the writing of this analysis, over 120 countries and independent jurisdictions have adopted comprehensive data protection laws, with another 40 currently considering draft acts or initiatives.[24]

In the MENA region, there is a growing interest in data protection and many neighbouring countries have already adopted laws, including Algeria, Bahrain, Lebanon, Morocco, Qatar, Turkey, and Tunisia as well as the UAE's Abu Dhabi Global Market and the Dubai International Financial Centre. Similar laws are currently being considered by Jordan, Kuwait, Oman, and Saudi Arabia. These laws all implement the international data protection principles, to some extent.

B. Balancing Privacy and Freedom of Expression and Information

The right to freedom of expression is a fundamental human right recognised in international human rights law. The full enjoyment of this right is central to achieving individual freedoms and to developing democracy. Freedom of expression is a necessary condition for the realisation of the principles of transparency and accountability that are, in turn, essential for the promotion and protection of all human rights.

As noted above, privacy and freedom of expression are intertwined rights in human rights law. They appear together in international instruments, national constitutions, and laws. They are mutually reinforcing.

Together they ensure the accountability of the state and other powerful actors to citizens. Freedom of expression and freedom of information allow individuals to investigate and challenge human rights abuses, including violations of privacy. Privacy allows

[20] EU General Data Protection Regulation (GDPR), Art. 5.

[21] Council of Europe, Modernised Convention for the Protection of Individuals with Regard to the Processing of Personal Data, Amending protocol to the Convention for the Protection of Individuals with Regard to the Processing of Personal Data, adopted by the Committee of Ministers at its 128th Session in Elsinore on 18 May 2018: https://www.coe.int/en/web/data-protection/convention108-and-protocol.

[22] Council of Europe, Modernised Convention for the Protection of Individuals with Regard to the Processing of Personal Data, Amending protocol to the Convention for the Protection of Individuals with Regard to the Processing of Personal Data, adopted by the Committee of Ministers at its 128th Session in Elsinore on 18 May 2018.

[23] See African Union Convention on Cyber-security and Personal Data Protection; ECOWAS Supplementary Act A/SA.1/01/10 on Personal Data Protection, OAS Principles on Privacy and Personal Data Protection in the Americas; OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (1980, updated 2013); APEC Privacy Framework, 2005; The Madrid Privacy Declaration, Global Privacy Standards for a Global World, 3 November 2009.

[24] See Greenleaf, Graham, Global Tables of Data Privacy Laws and Bills (6th Ed January 2019) (February 9, 2019). (2019) Supplement to 157 Privacy Laws & Business International Report (PLBIR) 16 pgs. Available at SSRN: https://ssrn.com/abstract=3380794; Banisar, David, National Comprehensive Data Protection/Privacy Laws and Bills 2018 (September 4, 2018). Available at https://ssrn.com/abstract=1951416 or http://dx.doi.org/10.2139/ssrn.1951416.

individuals to work in a space unhindered by authorities, and to develop their own voice. As a practical matter, limits on privacy affect the ability of the media to operate. Journalists are not able to effectively pursue investigations and receive information from confidential and other sources.[25] Data protection laws can support freedom of expression by placing limits on the unlawful collection of personal information for political purposes, such as bodies creating dossiers to put pressure on journalists and others.

There are some divergences. The tension between freedom of expression and the right to privacy can be exacerbated as personal information can be collected and made available across borders on an unprecedented scale and at minimal cost for both companies and states. At the same time, the application of data protection laws and other measures to protect the right to privacy can have a disproportionate impact on the legitimate exercise of freedom of expression.

Thus, as two equal human rights, it is essential that governments and courts balance the two in a fair manner without giving precedence to one over the other. International human rights law does not recognise a hierarchy of rights, in which one trumps the other. As the Vienna Declaration and Programme of Action adopted by the World Conference on Human Rights in 1993 states:

> All human rights are universal, indivisible, and interdependent and interrelated. The international community must treat human rights globally in a fair and equal manner, on the same footing, and with the same emphasis. While the significance of national and regional particularities and various historical, cultural, and religious backgrounds must be borne in mind, it is the duty of States, regardless of their political, economic, and cultural systems, to promote and protect all human rights and fundamental freedoms.[26]

The UN High Commissioner for Human Rights has stated:

> [A]ll human rights are equally important. The 1948 Universal Declaration of Human Rights makes it clear that human rights of all kinds—economic, political, civil, cultural, and social—are of equal validity and importance…. Human rights are also indivisible and interdependent. The principle of their indivisibility recognises that no human right is inherently inferior to any other.[27]

This approach of balancing rights has long been adopted by the European Court of Human Rights in cases involving privacy and freedom of expression:

> [W]hen verifying whether the authorities struck a fair balance between two protected values guaranteed by the Convention which may come into conflict with each other in this type of case, freedom of expression protected by Article 10 and the right to respect for private life enshrined in Article 8, the Court must balance the public interest in the publication of a photograph and the need to protect private life…. The balancing of individual interests, which may well be contradictory, is a difficult matter and Contracting States must have a broad margin of appreciation in this respect since the national authorities are in principle better placed than this Court to assess whether or not there is a "pressing social need" capable of justifying an interference with one of the rights guaranteed by the Convention.[28]

In a follow up case, the European Court of Human Rights clarified that when balancing the right to freedom of expression and the right to privacy, as a matter of principle, both rights deserved *equal respect.*[29] The Court went on to identify a number of relevant factors in balancing these rights, including:

- the contribution to a debate of public interest;
- how well known the person concerned is and the subject of the report;

[25] See e.g. IFEX Alert, Thirty IFEX members call on governments to respect fundamental human rights of free expression and privacy of communications, 5 June 2009. http://www.ifex.org/international/2009/06/05/ja_gm/.
[26] Vienna Declaration and Programme of Action, U.N. Doc A/CONF.157/23 (12 July 1993).
[27] Office of the United Nations High Commissioner for Human Rights, Frequently Asked Questions On A Human Rights-Based Approach To Development Cooperation, 2006.
[28] See e.g. Von Hannover v Germany, No 59320/00, 24 June 2004.
[29] European Court of Human Rights, *Von Hannover v. Germany No.2,* [GC], Nos. 40660/08&60641/08, para. 106, 2012.

- the prior conduct of the person concerned;
- content, form, and consequences of the publication; and
- circumstances in which photos were taken (where applicable).

A similar approach was adopted by the Inter-American Court of Human Rights which stated:[30]

> [T]he Court must find a balance between private life and freedom of expression that, not being absolute, are two fundamental rights guaranteed by the American Convention and of great importance in a democratic society. The Court recalls that every fundamental right is to be exercised with regard for other fundamental rights. This is a process of harmonisation in which the State has a key role in trying to determine responsibilities and impose sanctions as may be necessary to achieve such purpose.

The issue was also addressed by the African Union in the Declaration of Principles on Freedom of Expression in Africa, which state in Principle 7(2) that "Privacy laws shall not inhibit the dissemination of information of public interest".[31]

Data Protection and Freedom of Expression

The recognition of the need to reconcile competing rights has also been incorporated in international instruments on data protection. The CoE Modernised Convention 108's preamble states:

> Recalling that the right to protection of personal data is to be considered in respect of its role in society and that it has to be reconciled with other human rights and fundamental freedoms, including freedom of expression;

In the Explanatory Report, the CoE notes the need to balance freedom of expression and privacy rights:

> Taking into account the role of the right to protection of personal data in society, the preamble underlines the principle that the interests, rights, and fundamental freedoms of individuals have, where necessary, to be reconciled with each other. It is in order to maintain a careful balance between the different interests, rights, and fundamental freedoms that the Convention lays down certain conditions and restrictions with regard to the processing of information and the protection of personal data. The right to data protection is for instance to be considered alongside the right to 'freedom of expression' as laid down in Article 10 of the European Convention on Human Rights (ETS No. 5), which includes the freedom to hold opinions and to receive and impart information. Furthermore, the Convention confirms that the exercise of the right to data protection, which is not absolute, should notably not be used as a general means to prevent public access to official documents.[32]

This balance has also been addressed in other instruments. The European Commission in an impact assessment on the EU's General Data Protection Regulation (GDPR) noted that:

> Privacy and the protection of personal data… play a key role for the exercise of fundamental rights in a broader sense. Many of the fundamental freedoms can only be fully exercised if the individual is reassured that it is not subject of permanent surveillance and observation by authorities and other powerful organisations. Freedom of thought, freedom of expression, freedom of assembly and association, but also the freedom to conduct a business will not be exercised fully by all citizens in an environment where the individual feels that each of her or his moves,

[30] Inter-American Court of Human Rights, Case of Fontevecchia and d'Amico v. Argentina, Judgment of November 29, 2011 (Merits, Reparations, and Costs).

[31] Declaration of Principles on Freedom of Expression in Africa, African Commission on Human and Peoples' Rights, 32nd Session, 17 - 23 October, 2002: Banjul, The Gambia.

[32] Explanatory Report to the Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, 10 October 2018, paragraph 11 https://rm.coe.int/cets-223-explanatory-report-to-the-protocol-amending-the-convention-fo/16808ac91a.

acts, expressions and transactions is subject to scrutiny by others trying to control him or her. Exercise of these freedoms is crucial to maintain all fundamental rights.[33]

Thus, it is crucial to not treat the relationship of the two rights as a "zero sum" game, in which one "wins" over another, but to recognise their mutually supporting mechanisms.

III. The Legal Framework in Iran

In Iran, there are a number of legal instruments about privacy and data protection, both binding and non-binding, which provide some, but not comprehensive protections. Notably, these are the Islamic Republic of Iran Constitution, Electronic Commerce Law, Computer Crimes Law,[34] Islamic Penal Code and Civil Liability Act. Further, the right to privacy and data protection are mentioned in the Charter of Citizens' Rights which is a non-binding legal instrument for the protection of human rights. The relevant provisions and principles are summarised below.

However, there remains a significant gap relating to data protection. The Personal Data Protection and Safeguarding Draft Act constitutes the first attempt to introduce comprehensive legislation that regulates how personal information is used by organisations, businesses, or the government.

A. Constitution of 1979

The 1979 Constitution contains provisions on freedom of expression, access to information, and privacy.

Article 24 provides limited guarantees to the right to freedom of expression, as recognised by international law; it narrowly focuses on publications but does not expressly provide for a right to information. This right is limited by constitutional provisions that limit the freedom of expression on the basis of the protection of Islam or public rights.

Article 25 enshrines the right to privacy and data protection as qualified ones, by providing that the inspection of letters and the failure to deliver them, the recording and disclosure of telephone conversations, the disclosure of telegraphic and telex communications, censorship, or the wilful failure to transmit them, eavesdropping, and all forms of covert investigation are forbidden.

Article 3 on "state goals" requires that the government has a duty to use its resources for achieving several goals including reducing corruption and "raising the level of public awareness in all areas, through the proper use of the press, mass media, and other means".

B. Laws Protecting the Right to Privacy in Iran

The Computer Crimes Law that was enacted in 2009 contains several provisions ensuring the rights of individuals, including ensuring that consumers have privacy protections. Under this law, any oral or printed disclosure of personal information, fabrication of facts to publicly vilify the dignity of persons, or damage the reputation through insults and defamation, and casting aspersions on individuals are considered a breach of the reputation of others, and therefore treated as defamation.[35] It sets criminal penalties of imprisonment from one to five years and/or a fine for those who invade individual privacy through the use of electronic systems for "Every person who, without authority, steals data belonging to others, while the original data

[33] European Commission, Commission Staff Working Paper, Impact Assessment Accompanying the document Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), SEC(2012) 72 final, 25 January 2012.

[34] ARTICLE 19, Islamic Republic of Iran: Computer Crimes Law, Legal Analysis (2012) https://www.article19.org/data/files/medialibrary/2921/12-01-30-FINAL-iran-WEB%5B4%5D.pdf.

[35] Iran Computer Crimes Law, Chapters 4 and 5,

remains".[36] It should be noted that the aim of the law is to punish computer crimes, thus it applies to only the most serious actions.

The Electronic Commerce Law contains some provisions on data protection.[37] However, in the law, the protection of personal data is limited to e-consumers dealing with internet commerce. The Civil Code has no provisions protecting the right to privacy, while the 1960 Civil Liability Act states that "Any person who intentionally or due to his negligence, injures the life or health or property or freedom or prestige or commercial fame or any other right established for the individuals by virtue of law, as a result of which another one sustains materially or spiritually losses, shall be liable to compensate the damages arising out of his action".[38]

The Penal Code provides punishment for those who invade public ethics and dignity with imprisonment from three months to one year and with a fine, while the penalty is reduced from one to six months imprisonment if the offence is committed through the use of a telephone or communications systems without any fine to be imposed.[39]

The Electronic Commerce Law constitutes the main legislation in Iran to contain some provisions on privacy and data protection. However, for such law, the protection of personal data is limited to a specific context, namely in the context of e-consumers dealing with internet commerce.

C. Other Non-Binding Legal Instruments

In 2016, President Hassan Rouhani launched the Citizens' Rights Charter (the Charter). The Charter is in a non-binding document made up of 120 articles which incorporates many of the existing international civil, political, social, and economic rights obligations including freedom of expression, privacy, clean environment, and employment.

Chapter 9 includes seven sections on the rights to privacy and data protection. Article 37 in particular states that: "Searching, collecting, processing, using, and disclosing of letters, whether electronic or otherwise, personal information and data, as well other mail and telecommunications, such as telephone communications, faxes, wireless, private internet communications, and the like is prohibited, save pursuant to the law". The collection of private information of citizens is forbidden without the data subject's consent or when it is prescribed by law pursuant to Article 38. Article 39 continues, stating that "Citizens have the right to have their personal information, held by organs and natural persons and legal entities, protected and preserved".[40]

D. Problematic Provisions of Laws for Freedom of Expression

In Iran there are also other provisions that are relevant for freedom of expression. A revised version of the Islamic Penal Code (IPC) was introduced in 2013.[41] The new IPC retained numerous overbroad and vague restrictions on freedom of expression, which are not legitimate under international human rights law and facilitate the targeting of human rights defenders (HRDs), journalists, and dissenting or minority voices.[42]

Among the most problematic provisions misused in courts to restrict expression are:

[36] Iran Computer Crimes Law, Art. 12. See also Arts. 13, 14 and 16. Read ARTICLE 19's legal analysis https://www.article19.org/data/files/medialibrary/2921/12-01-30-FINAL-iran-WEB%5B4%5D.pdf.

[37] Electronic Commerce Law of the Islamic Republic of Iran. See in particular Arts. 58-61.

[38] Iran Civil Liability Code, Art. 1.

[39] Iran Penal Code (Fifth book, tazirāt), Arts. 640 and 641.

[40] Iran Charter of Citizens' Rights, Chapter 9 http://epub.citizensrights.ir/CitizensRightsEN.pdf.

[41] The Islamic Penal Code was revised in 2016. See the most updated version of the Islamic Penal Code here in the website for the Iranian parliament. http://rc.majlis.ir/fa/law/print_version/845048.

[42] "Codifying Repression: An Assessment of Iran's New Penal Code",," HRW. 29 August 2012. https://www.hrw.org/report/2012/08/28/codifying-repression/assessment-irans-new-penal-code.

- Book One, Chapter Nine, Article 286 defines the crime of efsad-e fel arz ("sowing corruption on earth"), which is punishable by death. This includes a set of ill-defined acts, such as "spreading lies", "establishment of, or aiding and abetting in, places of corruption and prostitution", or "disruption of the economic system" if these actions "cause severe disruption in the public order of the state and insecurity".[43]

- Book Two, Chapter Five, Article 262 vaguely criminalises anyone who "swears at or commits qazf"[44] against the Great Prophet of Islam" or other prophets and Imams, punishable by the death penalty.

Book Five contains key provisions criminalising expression lawful under international human rights law:

- Article 513 criminalises "insult" of the "sacred values of islam" and of religious leaders (punishable by between one and five years' imprisonment), with "insult" of the Prophet punishable by the death penalty;

- Article 514 criminalises "insult" of the Supreme Leader or the founder of the Islamic Republic, punishable by six months' to two years' imprisonment;[45]

- Article 500 criminalises "any type of propaganda against the [state] or in support of opposition groups and associations", punishable by imprisonment of three months to a year.[46] This is often abusively applied against journalists and human rights defenders;

- Article 698 criminalises anyone who causes "damage to someone" or disrupts "the opinion of the authorities or the public" through printed or written materials, punishable by two months' to two years' imprisonment, or up to 74 lashes; and[47]

- Article 618 criminalises "disrupting public order", punishable by three months' to a year's imprisonment, and up to 74 lashes.[48]

Penal Code Punishments

[43] "Article 286: "Any person, who extensively commits felony against the bodily entity of people, offencses against internal or international security of the state, spreading lies, disruption of the economic system of the state, arson and destruction of properties, distribution of poisonous and bacterial and dangerous materials, and establishment of, or aiding and abetting in, places of corruption and prostitution, [on a scale] that causes severe disruption in the public order of the state and insecurity, or causes harsh damage to the bodily entity of people or public or private properties, or causes distribution of corruption and prostitution on a large scale, shall be considered as mofsed-e-fel-arz [corrupt on earth] and shall be sentenced to death".

"Iran: Penal Code", RefWorld, available at: https://www.refworld.org/docid/518a19404.html.

[44] "Qafz" means the false accusation of sexual offencses.

[45] "Article 513 – Anyone who insults the sacred values of Islam or any of the Great Prophets or [twelve] Shi'ite Imams or the Holy Fatima, if considered as Saab ul-nabi [as having committed actions warranting the hadd punishment for insulting the Prophet], shall be executed; otherwise, they shall be sentenced to one to five years' imprisonment".

"Article 514 – Anyone who, by any means, insults Imam Khomeini, the founder of the Islamic Republic, and/or the Supreme Leader shall be sentenced to six months to two years' imprisonment".

"Islamic Penal Code of the Islamic Republic of Iran – Book Five", Iran Human Rights Documentation Center, available at: https://iranhrdc.org/islamic-penal-code-of-the-islamic-republic-of-iran-book-five/.

[46] "Article 500 – Anyone who engages in any type of propaganda against the Islamic Republic of Iran or in support of opposition groups and associations, shall be sentenced to three months to one year of imprisonment". -

[47] "Article 698, of the fifth book "Anyone who, with the intent to cause damage to someone or to disrupt the opinion of the authorities or the public by [sending] a letter or complaint or correspondence or petitions or reports or distribution of printed or written papers... shall be sentenced to two months' to two years' imprisonment or up to 74 lashes".

[48] "Article 618– Anyone who disrupts the order and public peace or prevents people from their business by crying out and creating a row and outrageous behavior or by assaulting other people shall be sentenced to three months to one year of imprisonment and up to 74 lashes".

The Personal Data and Safeguarding Draft Act calls on the use of the Fifth and Sixth Degree punishments from the Penal Code. It is essential to understand these punishments and their use under "necessary and proportionality" tests. The floggings under Sixth Degree punishments contravene both the ICCPR and the Convention Against Torture which both prohibit "torture and cruel, inhuman, or degrading treatment or punishment". Additionally, the Draft Act replicates the Islamic Penal Code's treatment of corporations (or legal persons) alongside with individuals (or natural persons), as seen in the punishments allocated to both entities under the fifth- and sixth-degree punishments applied to this Draft Law. In our section on the unclear application of the draft act, we note the problems when giving privacy rights to companies, a precedent set within this Islamic Penal Code.

Fifth Degree:

- Imprisonment from two to five years
- Fine from 80 million (80,000,000) Rials to 180 million (180,000,000) Rials
- Deprivation from social rights for five to 15 years
- Permanent ban from one or more professional or social activity (activities) for legal persons
- Permanent ban from public invitation to increase the capital for legal persons

Sixth Degree:

- Imprisonment from six months to two years
- Fine from 20 million (20,000,000) Rials to 80 million (80,000,000) Rials
- Flogging from 31 to 74 lashes and up to 99 lashes in indecent crimes
- Deprivation from social rights from six months to five years
- Publication of the final judgment in the media
- Ban from one or more professional or social activity (activities) for legal persons for up to five years
- Ban from public invitation to increase the capital for legal persons for up to five years
- Ban from drawing some commercial bills by legal persons for up to five years

The Computer Crimes Law[49] (CCL), adopted in 2010, continues to pose serious concern from the perspective of the right to freedom of expression and privacy. In particular:

- Article 14 of the CCL criminalises "producing, sending, publishing, distributing, saving or financially engaging in obscene content".
- Article 10 seeks to facilitate state surveillance by effectively prohibiting internet users and companies from using encryption, or protecting data, in a manner that would "deny access of authorised individuals to data, computer. and telecommunication systems".

[49] ARTICLE19's legal analysis https://www.article19.org/data/files/medialibrary/2921/12-01-30-FINAL-iran-WEB%5B4%5D.pdf.

- Article 21 imposes a sweeping requirement for ISPs to maintain records of internet traffic data and the personal information of their internet users, whilst Article 48 requires Internet Service Providers to record data from telephone conversations over the internet, in effect legalising mass surveillance.

These vague provisions give wide discretion to law enforcement authorities, including the hardline Revolutionary Guards (IRGC), and the Iranian Cyber Police (FATA)[50] to arbitrarily arrest and detain individuals on the basis of political motivations. Sanctions include prison sentences and fines, among others.

In June 2015, in a notable case, FATA targeted the administrator behind '23 anti-cultural groups on the Line and WhatsApp applications that published falsehoods and immoral content'[51] violating Article 14 of the CCL. This formed part of a pattern of targeting those sharing content via online platforms in the run up to the presidential elections and after, intended to deter Iranians from seeking and imparting crucial information online.

IV. Analysis of the Personal Data Protection and Safeguarding Draft Act

Overall, the Draft Act is poorly drafted and includes many inconsistent and conflicting provisions as well as being difficult to understand, which will seriously undermine its effectiveness. Given the lack of effective protections currently in Iranian law, it is crucial that these deficiencies be addressed to ensure that the law is compatible with international standards, fully protecting the data protection rights of all Iranians.

Further, it also does not achieve parity with European law, which is apparently a primary purpose of the Draft Act. In May 2018, when the GDPR entered into force, ICT Minister MJ Azari Jahromi announced that a draft data protection Draft Act was expected to be passed in the following months and that constructive talks were hoped for with the EU about mutual and legal assistance.[52] The Government in its press release announced that the Draft Act aimed to implement the constitutional right to privacy and to fill the legal gap existing in Iran.[53] According to the present analysis, the Draft Act falls short on both aspects as it does not include GDPR compliance, and is not a comprehensive data privacy regulation as it lacks general principles.

A. Lack of Principles

The first problem with the Draft Act is that the basic principles that govern the law are not clearly stated and outlined in the text. As illustrated above, the UN's 1990 Guidelines for the Regulation of Computerized Personal Data Files, adopted by General Assembly, requires six principles concerning the minimum guarantees that should be provided in national legislation. They are the principles of lawfulness and fairness, accuracy, purpose specification, interested-person access, non-discrimination, and security.

Only the transparency and security principles are clearly mentioned in Section 3 of the Draft Act. The principles of lawfulness and fairness, accuracy, purpose specification, interested-person access, and non-discrimination are not included in the draft. Such principles state that personal data must be processed lawfully and fairly for specified purposes and on the basis of the

[50] FATA was created in 2011 as the cyber crime unit of the Iranian national police force. The unit was created in compliance with the Cyber Crime Laws passed by the Iranian parliament in 2010. http://bbc.in/1VOXj2I.

[51] "The Arrest of 23 Admins of WhatsApp and Line groups," Iran Newspaper, 5 June 2015, http://www.iran-newspaper.com/newspaper/BlockPrint/67527

[52] MJ Azari Jahromi, ICT Minister of Iran tweeted on 25 May 2018: "Congratulations to @EU_Commission on the implementation of #GDPR, A comprehensive Data Protection rule! I'm also looking forward to passing the #DataProtection bill next months and conducting constructive talks with the EU about mutual legal & technical assistance". https://twitter.com/azarijahromi/status/999687318528778 24?s=20.

[53] See the Press Release announcing the Personal Data Protection and Safeguarding Draft Act: https://ito.gov.ir/news/-/view/انتشار-لایحه-پیش-نویس-حمایت-از-داده-های-حریم-خصوصی-در-فضای-مجازی/1409.

informed consent of the person concerned, or some other legitimate basis laid down by law. The approach adopted by the Draft Act requires a back and forth reading of the law which creates the risk of the law being inconsistently applied.

This is inconsistent with how nearly every data protection law in the world has been drafted and with international standards. In comparison, the Turkish Law on the Protection of Personal Data states in Article 4 that personal data will be processed in compliance with the principles of lawfulness and fairness, accuracy, purpose specification, storage limitation, and data minimisation.[54] The latter is a principle established under the General Data Privacy Regulation (GDPR) according to which personal data shall be adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed.[55] Similarly, data protection laws in Lebanon[56] and Algeria[57] have included the principles of purpose limitation, data minimisation, and accuracy.[58]

Recommendation

- The Draft Act should be redrafted to reorganise and streamline, fully incorporating the principles set out in international law in the text of the law and in a specific section placed after Section 2 that presents the "Definitions".

B. Unclear Application of the Draft Act

1. Absence of a Provision Establishing the Material and Territorial Scope of Application

Another significant omission in the Draft Act is the absence of any clear provision setting out the material and territorial scope of application. According to Article 1(b), the Draft Act will regulate "the processing of personal data". This provision outlines the aim of the law but the Draft Act presents no provision with regard its material scope. The material scope usually defines what types of processing of personal data the Draft Act applies to and which ones, conversely, are excluded. Data protection laws usually define its territorial scope of application in order to establish where persons as well as organisations have to be located in order to be obliged to comply with the law. The Draft Act does not present any such provisions.

This distinction has been put in place by the General Data Privacy Regulation (GDPR). As for the material scope, the Regulation is applicable to the processing completely or partly by automated means, such as, for instance, carried out with the use of computers containing digital databases. In addition, the processing of personal data by any other means is also regulated by the GDPR when these data are included in a filing system or are intended to be used in such a filing system, as stated in Article 2(1) of the GDPR. This can be the case when personal data are manually processed and are contained or are to be contained in a filing system with structured sets of personal data that are accessible in accordance with certain criteria, such as manual files printed on paper.

As for the territorial scope, According to Article 3(1) of the GDPR, it is applicable to the processing of personal data by controllers and processors with an establishment in the European Union. In this regard, it does not matter whether the actual processing is carried out in the Union or outside.

Importantly, Article 3(2) of the GDPR states that when controllers and processors are not established in the European Union but process personal data of individuals who are in the Union, the Regulation is applicable. Such processing activities must relate to the offering of goods or services for a payment or for free to these individuals or to the monitoring of the behaviour of these persons as long as this behaviour takes place in the European Union, as indicated in Article 3(2)(a) and (b) of the GDPR. Finally, the GDPR regulates the processing of personal data by controllers that are not established in the Union but somewhere

[54] Turkey, Law on the Protection of Personal Data, Art. 4.

[55] GDPR, Art. 5.

[56] Lebanon, Law n. 81 relating to Electronic Transactions and Personal Data, Art. 87.

[57] Algeria Law on the Protection of physical persons for the processing of personal data, 10 June 2018, Art. 9.

[58] Bahrain Law No. (30) for the year 2018 Issuing the Personal Data Protection Act, Art. 3.

else where laws of a EU Member State apply by virtue of public international law. This can be the case in diplomatic missions or consular posts of EU Member States.

According to international standards, it is crucial that the law applies to private as well as to public bodies. The UN Human Rights Committee and the UN General Assembly Declaration have both specifically stated that the right to privacy, as protected by data protection legislation, applies to information held by both private and public sector bodies. It is also generally recognised that the right to privacy creates positive obligations for states to also ensure that they adopt laws to protect all persons against attacks through legislation and actions. The UN HR Committee in General Comment No. 16 stated that:

> In the view of the Committee this right is required to be guaranteed against all such interferences and attacks whether they emanate from State authorities or from natural or legal persons. The obligations imposed by this article require the State to adopt legislative and other measures to give effect to the prohibition against such interferences and attacks as well as to the protection of this right.[59]

The UN General Assembly in the Guidelines on data protection for the Regulation of Computerized Personal Data Files, in relation to the "The Field of Application", stated that:

> The present principles should be made applicable, in the first instance, to all public and private computerised files as well as, by means of optional extension and subject to appropriate adjustments, to manual files. Special provision, also optional, might be made to extend all or part of the principles to files on legal persons particularly when they contain some information on individuals.[60]

Nearly every data protection law in the world applies to the processing of personal information of both public and private bodies. This includes those in the region. The 2018 Algerian Data Protection Law, passed in 2018, has a provision that explicitly states that it applies to both the private sector and public bodies.[61] In Qatar, the Protection of the Privacy of Personal Data Law states that the Act applies to "personal data upon e-processing thereof, when such Personal Data are received, collected, and mined in any other way in anticipation of e-processing the same".[62] Similarly, the long existing data protection laws in Morocco[63] and Tunisia also explicitly apply to public and private bodies.[64]

A clear definition of its scope of application will ensure legal certainty and accountability particularly in relation to public institutions when processing individual data. Therefore, the provision should be drafted in a way that clearly states that the law applies both to the private and public sector.

2. Discriminatory Application on Grounds of Citizenship

Article 3 of the Draft Act states that it applies to "Iranian citizens (individuals and corporations), public or private, whether their private data is being processed inside or outside Iran, and to foreign citizens (individuals and corporations), public or private, only if their data is processed by Iranian processors and controllers".

This provision is in violation of the principle of non-discrimination as it makes a distinction between data subjects according to their citizenship. The UN HR Committee in General Comment No. 16 states that:

---

[59] United Nations Human Rights Committee, General Comment No. 16: The right to respect of privacy, family, home and correspondence, and protection of honour and reputation (Art. 17), CCPR/C/GC/16, 4 August 1988.

[60] Guidelines for the Regulation of Computerized Personal Data Files, G.A. res. 45/95, 14 December 1990, http://www.un.org/documents/ga/res/45/a45r095.htm.

[61] Algeria Law on the Protection of physical persons for the processing of personal data, 10 June 2018, Art. 4.

[62] Qatar, Law No. 13 of 2016 Promulgating the Protection of the Privacy of Personal Data Law, Art. 2.

[63] Morocco, Law 09-08 on the protection of individuals with regards the processing of personal data, Art. 2.

[64] Tunisia, Law No. 2004-43 of 27 July 2004 on the Protection of Personal Data, Art. 2.

> Article 17 provides for the right of every person to be protected against arbitrary or unlawful interference with his privacy, family, home, or correspondence as well as against unlawful attacks on his honour and reputation.[65]

The Council of Europe Modernised Convention 108 on Data Protection also says that:

> The purpose of this Convention is to protect every individual, whatever his or her nationality or residence, with regard to the processing of their personal data, thereby contributing to respect for his or her human rights and fundamental freedoms, and in particular the right to privacy.[66]

The General Data Privacy Regulation (GDPR) applies to "the processing of personal data of data subjects who are in the Union". [67] The recently adopted Data Protection law in Bahrain also applies to natural persons who are also conducting business in the country or outside if it is "using means available" in Bahrain.[68]

3. The Draft Act Gives Privacy Rights to Companies

Further, an additional problem is that the Draft Act also gives the data protection rights of individuals to companies. This is a problematic aspect of the Draft Act that is against international standards. It should be borne in mind that the right to privacy and data protection are human rights that, as such, only apply to individuals. Companies, as legal entities, may have specific legal protections relating to trade secrets, intellectual property, and commercial confidentiality, as well as obligations protecting the privacy rights of their employees and customers, but should not be given rights to protect their privacy as they cannot possibly have any as merely legal entities.

In practice this could be extremely problematic, possibly requiring journalists to delete references to companies in news articles or provide information on their sources of information; requiring internet companies to censor articles revealing corruption or unethical practices; or limiting public bodies from revealing companies that have been investigated for violating laws.

As noted above, the UN Human Rights Committee has stated that article "provides for the right of every person" rather than legal entities. The resolution adopted by the General Assembly on 19 December 2016 affirms that "the same rights that people have offline must also be protected online, including the right to privacy".[69]

More recently, the GDPR has reaffirmed that:

> The protection afforded by this regulation should apply to natural persons, whatever their nationality or place of residence, in relation to the processing of their personal data. This regulation does not cover the processing of personal data which concerns legal persons and in particular undertakings established as legal persons, including the name and the form of the legal person and the contact details of the legal person.[70]

Furthermore, the GDPR defines personal data as:

> 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

[65] United Nations Human Rights Committee, General Comment No. 16: The right to respect of privacy, family, home and correspondence, and protection of honour and reputation (Art. 17), CCPR/C/GC/16, 4 August 1988.

[66] Council of Europe, Modernised Convention for the Protection of Individuals with Regard to the Processing of Personal Data, Amending protocol to the Convention for the Protection of Individuals with Regard to the Processing of Personal Data, adopted by the Committee of Ministers at its 128th Session in Elsinore on 18 May 2018, Art. 11. https://rm.coe.int/convention-108-convention-for-the-protection-of-individuals-with-regar/16808b36f1.

[67] EU General Data Protection Regulation (GDPR), Art. 3.2.

[68] Bahrain Law No. (30) for the year 2018 Issuing the Personal Data Protection Act, Art. 2.

[69] The right to privacy in the digital age, G.A. res. 71/199, 19 December 2016, par. 3.

[70] GDPR, Recital 14. See also Arts. 1 and 2.

> 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.[71]

Recommendations

- The Draft Act should include a specific provision regulating its material and territorial scope of application. The provision should clearly state that it will apply to all government entities as well as to private bodies. Currently, these rights are not adequately protected by other Iranian legislation. These changes should also be harmonised with the Publication and Free Access to Information Act of 2009.

- Article 3 should be redrafted to put it in line with the principle of non-discrimination in order to apply to every individual and not just citizens and foreign citizens whose data are processed in the territory of Iran. In its current formulation, differentiating citizens and foreign citizens, as well as the exclusion of stateless citizens as regards the scope of application of the Draft Act violates international human rights obligations.

- The Draft Act should specifically remove application of privacy and data protection to corporations.

C. Impacts on Freedom of Expression and Information

Another significant problem with the Draft Act is its relationship to freedom of expression. As noted above, under international law, states should ensure that the enforcement of data protection rights includes broad exemptions or limitations in order to ensure the exercise of freedom of expression.

The Office of the United Nations High Commissioner for Human Rights in their report "The Right to Privacy in the Digital Age", presented to the Human Rights Council in August 2018, emphasised that:

> It is important that the legal framework ensures that those rights (i.e. privacy and data protection) do not unduly limit the right to freedom of expression, including processing of personal data for journalistic, artistic, and academic purposes.[72]

The European Court of Justice has long ruled that states must develop a "fair balance" between the right to privacy and freedom of expression based on the principle of proportionality. As noted by the ECJ in a 2008 case:

> In order to take account of the importance of the right to freedom of expression in every democratic society, it is necessary, first, to interpret notions relating to that freedom, such as journalism, broadly. Secondly, and in order to achieve a balance between the two fundamental rights, the protection of the fundamental right to privacy requires that the derogations and limitations in relation to the protection of data provided for in the chapters of the directive referred to above must apply only in so far as is strictly necessary.

The Draft Act, in its introduction, recalls several constitutional provisions, namely Chapter Three in general and some provisions in particular, that the Draft Act aims to implement. Worryingly, the right to freedom of expression enshrined in Article 24 of the Constitution is not mentioned among the other rights such as the right to privacy. As explained above, the two rights are mutually supportive. They should be balanced in a fair manner without giving precedence to one over the other. International human rights law does not recognise a hierarchy of rights. Besides, it is crucial to recognise the importance of freedom of

[71] GDPR, Recital 14. See also Art. 4.

[72] Annual report of the United Nations High Commissioner for Human Rights and reports of the Office of the High Commissioner and the Secretary-General, A/HRC/39/29 of 3 August 2018. https://www.ohchr.org/Documents/Issues/DigitalAge/ReportPrivacyinDigitalAge/A_HRC_39_29_EN.docx.

expression, as the unlawful collection and processing of personal data—particularly if it involves journalists—would affect the ability of the media to operate and to effectively pursue investigations and receive information from confidential and other sources.

1. Failure to Include Journalistic, Artistic, Literary, and Other Cultural Exemptions

In the Draft Act, Article 12 states that the processing of private data within the framework of relevant laws without their consent is allowed in several circumstances. However, there is no mention of any exemption for artistic, literary, and cultural purposes. This is a serious shortcoming in the proposed law. More worryingly, the processing for journalistic purposes is not considered at all. The Draft Act further fails to recognise freedom of expression interests, such as the free exchange of information by individuals, as well as the aforementioned artistic, literary, and cultural purposes.

Nearly all countries around the world that have adopted data protection acts have specifically included a clear exemption for journalistic, artistic, literary, and other cultural purposes which allows for the rules limiting processing to be waived for those purposes. There should also be exemptions for the discharge of any legal obligation to make information publicly available, such as the maintenance of archives for historical or other public interest purposes, or under right to information laws. Moreover, such exemptions or limitations must be interpreted broadly so as to give meaningful effect to the rights to freedom of expression and to information.

This exemption was first set out in Article 9 of the EU Data Protection Directive 95/45, the old European legal framework with regards the processing of personal data. The European Court of Justice, in the case cited above stated that its provisions applied beyond just the official media: "the exemptions and derogations provided for in Article 9 of the directive apply not only to media undertakings but also to every person engaged in journalism". It stated that the journalistic exemption applied "if their object is the disclosure to the public of information, opinions, or ideas, irrespective of the medium which is used to transmit them. They are not limited to media undertakings and may be undertaken for profit-making purposes".

The breadth of protected freedom of expression related activities has been extended with the adoption of the Regulation on Data Protection (GDPR). Article 85 on the "processing of personal data and freedom of expression and information" states that:

> 1. The national law of the member state shall reconcile the right of protection of personal data pursuant to this Regulation with the right of freedom of expression and information, including the processing of personal data for journalistic purposes and the purposes of academic, artistic, or literary expression.
>
> 2. For the processing of personal data carried out for journalistic purposes or the purpose of academic artistic or literary expression, Member States shall provide for exemptions or derogations from the provisions in Chapter II (principles), Chapter III (rights of the data subject), Chapter IV (controller and processor), Chapter V (transfer of personal data to third countries or international organisations), Chapter VI (independent supervisory authorities), Chapter VII (co-operation and consistency) if they are necessary to reconcile the right to the protection of personal data with the freedom of expression and information (...).

Specific protections for freedom of expression have also been incorporated in the Modernised Council of Europe Convention 108 on Data Protection. Article 11 (b) states that Member States must incorporate an exemption when it is necessary for the "the protection of the data subject or the rights and fundamental freedoms of others, notably freedom of expression".[73] The commentaries on the Convention further explained that:

> Littera b. concerns the rights and fundamental freedoms of private parties, such as those of the data subject himself or herself (for example when a data subject's vital interests are threatened because he or she is missing) or of third parties, such as freedom of expression, including freedom of journalistic, academic, artistic, or literary expression,

[73] Council of Europe, Modernised Convention for the Protection of Individuals with Regard to the Processing of Personal Data, Amending protocol to the Convention for the Protection of Individuals with Regard to the Processing of Personal Data, adopted by the Committee of Ministers at its 128th Session in Elsinore on 18 May 2018, Art. 11. https://rm.coe.int/convention-108-convention-for-the-protection-of-individuals-with-regar/16808b36f1.

> and the right to receive and impart information, confidentiality of correspondence and communications, or business or commercial secrecy and other legally protected secrets. This should apply in particular to processing of personal data in the audio-visual field and in news archives and press libraries. In order to take account of the importance of the right to freedom of expression in every democratic society, it is necessary to interpret notions relating to that freedom, such as journalism, broadly.

At the domestic level, a journalistic exemption has been incorporated in most data protection laws around the world including those in the region. The Data Protection Law in Turkey provides for exceptions with regards personal data processed within the scope of freedom of expression.[74] In Bahrain,[75] Lebanon,[76] and Algeria,[77] the data protection laws exclude from their scope of application the processing of personal data for the purposes of the exercise of journalistic activity.

2. The Right to be Forgotten

Article 9 of the Draft Law states that, "Requests to process or cease to process personal data can be done with the aim of forgetting provided that there is no other beneficiary ".

In our understanding, this provision constitutes an attempt to introduce the "right to be forgotten" in the Draft Act and into Iranian law. The provision lacks clarity in establishing the right to make requests to process or stop processing with the "aim of forgetting" without establishing any limits. It appears to give any person, no matter their official or public position or the public interest, an absolute right in demanding that information related to their actions be deleted.

The right to be forgotten was first examined by the Court of Justice of the European Union (CJEU) in the *Google Spain* case. Under this right, data subjects have a right to request Google and other search engines operating in the EU to de-list links to results generated by a search for their name except when there were public interest considerations.

Under international law, the right to be forgotten is not an absolute right and freedom of expression must be considered. The UN Special Rapporteur on Freedom of Opinion and Expression, in his 2016 report, provided a global review of issues affecting free expression on the internet, including the right to be forgotten, and reminded states of their obligations under the ICCPR:

> Any demands, requests and other measures to take down digital content or access customer information must be based on validly enacted law, subject to external and independent oversight, and demonstrate a necessary and proportionate means of achieving one or more aims under article 19(3) of the International Covenant on Civil and Political Rights. Particularly in the context of regulating the private sector, State laws and policies must be transparently adopted and implemented.[78]

In the CJEU's judgement mentioned above, the Court explicitly clarified that the right to be forgotten is not absolute but will always need to be balanced against other fundamental rights, such as freedom of expression and of the media. It held in particular:

> As the data subject may, in the light of his fundamental rights under Articles 7 and 8 of the Charter, request that the information in question no longer be made available to the general public by its inclusion in such a list of results, it should be held… that those rights override, as a rule, not only the economic interest of the operator of the search engine but also the interest of the general public in finding that information upon a search relating to the data subject's name. However, that would not be the case if it appeared, for particular reasons, such as the role played by the data

[74] Turkey Law on the Protection of Personal Data, Art 28 (d).

[75] Bahrain Law No. (30) for the year 2018 Issuing the Personal Data Protection Act, Art. 6.

[76] Lebanon Law n. 81 Relating to Electronic Transactions and Personal Data, Art. 105.

[77] Algeria Law on the Protection of physical persons for the processing of personal data, 10 June 2018, Art. 29.

[78] Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, David Kaye, to the Human Rights Council, 11 May 2016.

> subject in public life, that the interference with his fundamental rights is justified by the preponderant interest of the general public in having, on account of inclusion in the list of results, access to the information in question.[79]

The Article 29 Working Party of EU Data Protection Authorities (now the European Data Protection Board) has also issued guidance elaborating on the need to recognise freedom of expression when applying the right:

> [T]here is also an interest of internet users in receiving the information using the search engines. In that sense, the fundamental right of freedom of expression, understood as "the freedom to receive and impart information and ideas" in Article 11 of the European Charter of Fundamental Rights, has to be taken into consideration when assessing data subjects' requests…. Search engines must take the interest of the public into account in having access to the information in their assessment of the circumstances surrounding each request. Results should not be de-listed if the interest of the public in having access to that information prevails. [80]

The guidelines set out criteria for consideration, including:

- Does the data subject play a role in public life?
- Is the data subject a public figure?
- Is the data accurate?
- Does the data relate to the working life of the data subject?
- Was the original content published in the context of journalistic purposes?

The EU GDPR further clarified the right in two provisions in the Right to Erasure section. Under Article 17(3)(a), the right of erasure shall not apply "for exercising the right of freedom of expression and information". Further, it is also exempt under 17(3)(c) "for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes… in so far as the right referred to in paragraph 1 is likely to render impossible or seriously impair the achievement of the objectives of that processing". Recital 65 emphasises the freedom of expression and archive rights:

> The further retention of the personal data should be lawful where it is necessary, for exercising the right of freedom of expression and information, for compliance with a legal obligation, for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller, on the grounds of public interest in the area of public health, for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes.

Similarly, the Explanatory Report for the modernised version of Convention 108 notes that the right to erasure and other rights are not unlimited:

> These rights may have to be reconciled with other rights and legitimate interests. They can, in accordance with Article 11, be limited only where this is provided for by law and constitutes a necessary and proportionate measure in a democratic society.

ARTICLE 19, in a policy paper on the "right to be forgotten", has proposed a seven-part test:

- Whether the information in question is of a private nature;
- Whether the applicant had a reasonable expectation of privacy, including the consideration of issues such as prior conduct, consent to publication, or prior existence of the information in the public domain;
- Whether the information at issue is in the public interest;
- Whether the information at issue pertains to a public figure;

[79] Case C-131/14, Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González, 13 May 2014, p 81.

[80] Article 29 Data Protection Working Party, Guidelines on the Implementation of the Court of Justice of the European Union Judgment on Google Spain And Inc V. Agencia Española De Protección De Datos (Aepd) and Mario Costeja González C-131/12 adopted on 26 November 2014 https://www.pdpjournals.com/docs/88502.pdf.

- Whether the information is part of the public record;
- Whether the applicant has demonstrated substantial harm; and
- How recent the information is and whether it retains public interest value.[81]

Beyond the test, ARTICLE 19 recommends procedural protections on the implementation of the right:

- The courts should be tasked with balancing the relevant interests at issue rather than search engines or data protection authorities.

- Content providers should be notified that a "right to be forgotten" request has been made in relation to their content and be able to challenge such requests.

- Relevant providers, public authorities and the courts should be required to publish transparency reports about 'RTBF' requests.

3. Localisation Requirements

The Draft Act also appears to limit Iranians' access to websites and common services available on the internet, in violation of individuals' freedom of expression, in the name of data protection.

Chapter 3, Section 5 of the law sets limits on "foreign-based processing". Article 38 states:

> For the processing of personal data of Iranian citizens, the following conditions need to be met:
>
> A) They can only be stored in the data centers located in the sovereign realm of the Islamic Republic of Iran or the foreign-based data centers approved by the relevant authorities.

This section is problematic from a freedom of expression standpoint. Such "data localisation" laws have been used in a number of jurisdictions as a pretense to limit access to social media platforms. In Russia, they are being used to limit access to Twitter and Facebook. In addition, forced data localisation makes it easier for authorities to access the private communications of dissidents and others. The provision also violates the principle of non-discrimination by referring to the personal data of Iranian citizens.[82] It is also unclear which process is to be followed for localisation as point B mentions the "issuing of a license by relevant authorities" without clarifying which ones are involved. The provision goes on by saying that personal data shall be transferred to foreign countries via "trustable communication networks" without providing any definition of what this means under the law. The Special Rapporteur for Freedom of Expression and Information of the Organization of American States has noted the problems with localisation:

> The forced localisation of data may be a mechanism for the restriction of freedom of expression for various reasons. First, the forced localisation of internet intermediaries substantially reduces the supply of services and platforms that users can freely access. It is important to note that the freedom to choose which services and platforms to access is a prerogative of users in the exercise of their freedom of expression and cannot be restricted by governments without violating the unique nature of the internet as a free, open, and decentralised medium. This opportunity to choose is essential in many States in which individuals are subjected to arbitrary interference in their privacy by the States. In such cases, the opportunity to choose the uninhibited exercise of freedom of expression. In other words, the absence of adequate local laws or public policies for the protection of data could cause greater insecurity in the access to data if they are located in a specific country, as opposed to being stored in multiple locations or in places that offer better safeguards.

[81] ARTICLE 19, The "Right to be Forgotten": remembering Freedom of Expression (2016) available here https://www.article19.org/data/files/The_right_to_be_forgotten_A5_EHH_HYPERLINKS.pdf.

[82] For the distinction posed by the Draft Act between Iranian citizens and foreign citizens see S

> … In addition, requiring Internet Service Providers to store data locally can create a barrier to entry into the market for new platforms and services. This would negatively affect the freedom of expression of users, who will see their access to resources for research, education, and communication reduced. Indeed, meeting the requirement of data localisation is complex and costly, and harms individual users or new initiatives by potentially depriving them of the conditions of interoperability necessary to connect globally. Freedom of expression and democracy assume the free flow of information and require the prevention of measures that create fragmentation in the internet.
>
> … In this respect, the exercise of freedom of expression requires conditions that encourage—rather than discourage—user access to a plurality and diversity of media.[83]

The UN Special Rapporteur for Freedom of Expression and Opinion, in his 2016 report, recommended "It will be particularly critical for States to avoid adopting legal rules that implicate digital actors—including, but not limited to, data localisation standards, intermediary liability and internet security—that undermine the freedom of expression…"[84]

In comparison, the GDPR does not impose any requirement that the data be located in an EU Member State. It requires that the state have adequate data protection provisions similar to the GDPR; personal data can be transferred to third countries under the condition that the level of protection of natural persons guaranteed by the Regulation is not undermined. The two relevant sections state:

> Article 45: A transfer of personal data to a third country or an international organisation may take place where the Commission has decided that the third country, a territory, or one or more specified sectors within that third country, or the international organisation in question ensures an adequate level of protection. Such a transfer shall not require any specific authorisation.
>
> Article 46: In the absence of an adequacy decision by the Commission, a controller or processor may transfer personal data to a third country or an international organisation only if the controller or processor has provided appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available.

Other countries in the region have also followed this approach. In Turkey, personal data can be transferred abroad if sufficient protection is provided in the foreign country where data is to be transferred or the Board has authorised such transfer, where sufficient protection is not provided.[85] The same principles also apply in Tunisia.[86]

4. Failure to Balance Data Protection with the Right to Information

The public right of access to information held by public bodies is a fundamental aspect of the right of freedom of expression[87] The right of access to information and data protection often play complementary roles. They both are focussed on ensuring accountability of powerful institutions to individuals in the information age. Michel Gentot, the former President of the French National Commission for Liberties and Informatics (CNIL), stated "FOI and Data Protection" are "two forms of protection against the Leviathan state that have the aim of restoring the balance between the citizen and the state".

International law clearly requires that the right of access to information is reconciled with the right of privacy. As with freedom of expression, any limitations must be established in law, necessary, and proportionate.[88]

---

[83] Office of the Special Rapporteur for Freedom of Expression Inter-American Commission on Human Rights, Freedom of Expression and the Internet, 2013.

[84] Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, A/71/373, 6 September 2016.

[85] Turkey Law on the Protection of Personal Data, Article 9.

[86] Tunisia Organic Act 2004-63 on the Protection of Personal Data, 27 July 2004, Art. 51.

[87] UN Human Rights Committee, General Comment 34.

[88] Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue, A/68/362, 4 September 2013.

The Council of Europe stated in a 1986 Resolution that they are "not mutually distinct but form part of the overall information policy in society".[89] The Modernised Council of Europe Convention 108 includes a specific reference to public access to information in its recitals:

> Considering that this Convention permits account to be taken, in the implementation of the rules laid down therein, of the principle of the right of access to official documents;

The explanatory note to the revised convention states:

> Furthermore, the Convention confirms that the exercise of the right to data protection, which is not absolute, should notably not be used as a general means to prevent public access to official documents.

The EU GDPR further extends this recognition. Article 86 states:

> Personal data in official documents held by a public authority or a public body or a private body for the performance of a task carried out in the public interest may be disclosed by the authority or body in accordance with Union or Member State law to which the public authority or body is subject in order to reconcile public access to official documents with the right to the protection of personal data pursuant to this Regulation.

Many national data protection laws in Europe and around the world have a specific recognition of the right to information. In Ireland, Article 44 of the Data Protection Act 2018, implementing the GDPR states:

> (1) For the purposes of Article 86, personal data contained in a record may be disclosed where a request for access to the record is granted under and in accordance with the Act of 2014 pursuant to an FOI request.
>
> (2) For the purposes of Article 86, personal data contained in environmental information may be disclosed where the information is made available under and in accordance with the Access to Information on the Environment Regulations pursuant to a request within the meaning of those Regulations.

In South Africa, the Promotion of Access to Information Act requires that disclosure of information must be declined if it "would involve the unreasonable disclosure of personal information about a third party, including a deceased individual". However, the information can be disclosed if it is:

> about an individual who is or was an official of a public body and which relates to the position or functions of the individual, including, but not limited to:
>
> (i) the fact that the individual is or was an official of that public body;
> (ii) the title, work address, work phone number and other similar particulars of the individual;
> (iii) the classification, salary scale, or remuneration and responsibilities of the position held or services performed by the individual; and
> (iv) the name of the individual on a record prepared by the individual in the course of employment.[90]

It is important to ensure that public registers and other information relating to the operation of government or in the public interest also remain public, and are not unnecessarily restricted in the name of data protection. These records can be quite crucial to ensuring accountability, including public information procurement, public registers of company owners, information on company officials meeting with public officials to influence their decisions, recipients of subsidies, and more.

Thus, it is also necessary that the Draft Act fully recognise the public interest when there is a request to access records which contain personal information of any kind about private individuals.

[89] Council of Europe Recommendation 1037 On Data Protection and Freedom of Information (1986).
[90] Promotion of Access to Information Act, §34.

They should be subject to an assessment of harm which must be serious either immediately or subsequently. They should also be subject to an evaluation of public interest for providing or denying information for each request separately, which considers the relative interests that need to be protected and the purpose of the access request.

There have been a number of decisions in the context of access to information[91] on how to balance the two rights. The UK Information Commissioner has noted that:

> The public interest can cover a wide range of values and principles relating to the public good, or what is in the best interests of society. Thus, for example, there is a public interest in transparency and accountability, to promote public understanding, and to safeguard democratic processes. There is a public interest in good decision-making by public bodies, in upholding standards of integrity, in ensuring justice and fair treatment for all, in securing the best use of public resources and in ensuring fair commercial competition in a mixed economy. This is not a complete list; the public interest can take many forms.

The Commentaries on the revised version of the CoE Modernised Convention 108 explain that the Convention confirms that the exercise of the right to data protection, which is not absolute, should notably not be used as a general means to prevent public access to official documents.[92]

Unfortunately, the Draft Act fails to take into consideration and to balance the right to data protection and the right of access to information.

In Iran, the right to information is enabled by the Publication and Free Access to Information Act. Under Article 14, information relating to privacy or personal data can be withheld when it would harm the person's interest. The exemptions are not considered absolute[93].

However, it should be noted that the Publication and Free Access to Information Act also falls short of balancing the right to privacy and right to information as described above. Under Article 9 of the bylaw:

"[i]nstitutions subject to this Act are prohibited from publishing or providing private information that is considered restricted by law unless ordered otherwise by law."[94]

The definition of such private information does not clarify that under best practice and public interest, such personal information should not apply to names of officials or their official activities. The Publication and Free Access to Information Act also currently provides privacy protection for such information which is necessary to be published because of public interest. For example, under the Yemen right to information law (2012), personal information can be released if it is "connected to the duty or function or public office held by that individual."[95]

In contrast, the Draft Data Protection Act makes no reference to the Publication and Free Access to Information Act. Article 12 of the Draft Act lists several conditions under which the processing of private data within the framework of relevant laws without data subjects' consent is allowed. It mentions in particular cases when it is necessary for safeguarding the person's reputation, life, or property or for the reputation and life of another person or preventing acute financial damage to them. There is no exemption for enabling the right to information and considering the public interest in the release of information. This provision appears to set up a conflict of laws with the Publication and Free Access to Information Act.

---

[91] Inter-American Court of Human Rights, Case of Claude-Reyes et al. v. Chile Judgment of September 19, 2006.

[92] Explanatory Report to the Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, 10 October 2018, par 11.

[93] This simply means that exemptions must have limited scope, be clearly and narrowly down and subject to strict harm and public interest test. This is important to ensure that public registers and other information relating to the operation of government or in the public interest also remain public, and are not unnecessarily restricted in the name of data protection.

[94] Executive Bylaw of Article 9 of The Publication and Free Access to Information Act, Proclamation No: H51979T/84348, 21 September 2015

[95] Law (13) for the Year 2012 Regarding the Right of Access to Information, §25(B).

As a primary step, the data protection Draft Act should be amended to include an explicit exemption for personal information relating to public activities of public officials or others acting under public authority or spending public money. Such amendment will reflect the right of information enshrined in the Publication and Free Access to Information Act.

In this regard, the Draft Act risks being a step backwards and undermining the rights given under the Publication and Free Access to Information Act and protected by the Constitution.

Recommendations

- The Introduction should be redrafted in order to recall also the right to freedom of expression as enshrined in the Constitution and to mention the Charter of Citizens' Rights that provides framework for the protection of the right to freedom of expression, the right to access to information, the right to privacy and to data protection in Iran. The Draft Act should take into account Iran's responsibilities as State party to the ICCPR, most notably Articles 17 (the right to privacy) and 19 (the right to freedom of expression).

- Revise Article 12 in order to include an exemption to processing that is intended to communicating information to the public, ideas, or opinions of general interest including for journalistic purposes and the purposes of academic, artistic or literary expression. Article 12 should also include assurances that due process is followed when accessing data without consent by better clarifying what the purpose of preventing or answering threats to order, security or public safety means. Such terms could also be defined in Article 2 which presents "Definitions" in order not to empower authorities to abuse rights of individuals, especially in efforts to repress and prosecute human rights defenders, minorities, journalists, bloggers and activists.

- The Draft Act should also ensure that journalists and other public interest communicators—including non-governmental organisations that are publishing information of public interest—are protected from being forced to reveal the sources of their information.

- Ensure that any rules on the deletion of public information are balanced with freedom of expression and the public interest in accessing information and historical archiving by incorporating ARTICLE 19's seven-part test to the "right to be forgotten" into Article 9.

- Remove requirements that all personal data be subject to data localisation. Replace with ensuring adequacy of data protection in foreign jurisdiction.

- Amend Article 12 to include an explicit exemption for personal information relating to public activities of public officials or others acting under public authority or spending public money to reflect the right of information enshrined in the Constitution and the public interest in obtaining information.

- The Draft Act should specifically recognise the public interest provisions granted by the Publication and Free Access to Information Act to public bodies and ensure that the public interest is considered in any request.

D. Limitations on Access Rights

The right of individuals to obtain access to personal information about themselves held by third parties (known usually as the "Subject access right" or "Interested-Person Access") including public bodies and private companies is a fundamental right recognised under international law. The UN Human Rights Committee in General Comment 16 noted that the right is necessary in order to ensure respect of the right to privacy:

> "In order to have the most effective protection of his private life, every individual should have the right to ascertain in an intelligible form, whether, and if so, what personal data is stored in automatic data files, and for what purposes. Every individual should also be able to ascertain which public authorities or private individuals or bodies control or

> may control their files. If such files contain incorrect personal data or have been collected or processed contrary to the provisions of the law, every individual should have the right to request rectification or elimination".[96]

This right has been widely incorporated into international law, as well as in major regional agreements on data protection. The European Court of Human Rights has described the right of access as a "vital interest, protected by the Convention".[97] In the GDPR, every individual has a strong right of access. As stated in the recitals:

> A data subject should have the right of access to personal data which have been collected concerning him or her, and to exercise that right easily and at reasonable intervals, in order to be aware of, and verify, the lawfulness of the processing. This includes the right for data subjects to have access to data concerning their health, for example the data in their medical records containing information such as diagnoses, examination results, assessments by treating physicians, and any treatment or interventions provided. Every data subject should therefore have the right to know and obtain communication in particular with regard to the purposes for which the personal data are processed, where possible the period for which the personal data are processed, the recipients of the personal data, the logic involved in any automatic personal data processing and, at least when based on profiling, the consequences of such processing. Where possible, the controller should be able to provide remote access to a secure system which would provide the data subject with direct access to his or her personal data. That right should not adversely affect the rights or freedoms of others, including trade secrets or intellectual property and in particular the copyright protecting the software. However, the result of those considerations should not be a refusal to provide all information to the data subject. Where the controller processes a large quantity of information concerning the data subject, the controller should be able to request that, before the information is delivered, the data subject specify the information or processing activities to which the request relates.[98]

The Citizen Charter[99] also outlines this in Article 31:

"Citizens have the right to access their personal data collected and kept by persons and institutions providing public services, and to request correction of such data, should they find it to be incorrect. Personal information pertaining to individuals shall not be placed at the disposal of others, save pursuant to the law or with the consent of the individuals themselves."[100]

The Publication and Free Access to Information Act prescribes rights to access personal information. Requests for information of this type are the same as for other types of information described in the act. However, under Article 6 of the Act only the person whose information is being requested or their legal representative can ask for such personal information.

Under the Article 15 of the Article 8 bylaw of The Publication and Free Access to Information Act, the Iran Information Technology Organization is obliged to provide, within six months and in collaboration with the national post, an operational system of citizens' national files for access. [Executive Bylaw of Article 8 of The Publication and Free Access to Information Act, Proclamation No: H51979T/84348, 21 September 2015]

---

[96] General Comment 16, ibid at §10.

[97] *Gaskin v. the United Kingdom*, 7 July 1989, § 49, Series A no. 160; *M.G. v. the United Kingdom*, no. 39393/98, § 27, 24 September 2002; *Odièvre v. France*[GC], no. 42326/98, § 41-47, ECHR 2003III); *Guerra and Others v. Italy*, 19 February 1998.

[98] GDPR, Recital 63.

[99] In 2016, President Hassan Rouhani launched the Citizens' Rights Charter (the Charter). The Charter is in a non-binding document made up of 120 articles which incorporates many of the existing international civil and political and social and economic rights obligations including freedom of expression, privacy, clean environment, and employment. Critics, including Nobel Laureate Shirin Ebadi, have described the Charter as being redundant12 but as described below, it does include new rights relating to access to information not in the Constitution. In 2017 the administration began proposing bills to the Parliament to make its provisions binding in sections.

[100] Translation of draft text available at http://epub.citizensrights.ir/CitizensRightsEN.pdf ; Farsi version http://rouhani.ir/files/CitizensRights.pdf.

In comparison, the Draft Act has a limited provision, which is largely unclear in its application and limitations. Article 10 of the Draft Act states that "the person has the right to access their own data with the aim of processing them". There are two limitations to the access:

- Data does not include public classified information or other people's private data; and
- Referability of data is not disturbed.

The provision does not define what "public classified information" means.

Further, Article 26 obligates the processor to provide information on the purposes, sources, obligations, and uses of the information but not clearly the data itself.

Significantly, in the Draft Act the right to correction is not specifically granted. General Comment No. 16 states:

> If such files contain incorrect personal data or have been collected or processed contrary to the provisions of the law, every individual should have the right to request rectification or elimination.[101]

Under the GDPR, the controller should also "use all reasonable measures to verify the identity of a data subject who requests access, in particular in the context of online services and online identifiers. A controller should not retain personal data for the sole purpose of being able to react to potential requests".[102] It also provides for a "right to rectification", namely "the right to obtain from the controller without undue delay the rectification of inaccurate personal data concerning him or her. Taking into account the purposes of the processing, the data subject shall have the right to have incomplete personal data completed, including by means of providing a supplementary statement".[103]

Recommendations

- Clarify Article 10 to ensure that persons have full and free access to their personal information held by third parties except in limited instances allowed under international law, most notably General Comment No. 16. Define what "public classified information" means under Article 10.
- Grant data subjects a right of correction.

E. Independence of the Data Protection Commission and Other Oversight Bodies

ARTICLE 19 is highly concerned about the independence of the body in charge of overseeing the application of the Personal Data Protection and Safeguarding Draft Act. This is a crucial aspect of the Draft Act as the guarantee of independence of national data protection supervisory authorities is intended to ensure the effectiveness and reliability of the supervision of compliance with the provisions on the right to data protection. It follows that, when carrying out their duties, supervisory authorities must act objectively and impartially without any external influence, including the direct or indirect influence of the government.

1. Structure and Powers

The Draft Act sets out a complex structure of entities that are in charge of the implementation of the data protection rules. The five bodies involved are: the Data Protection Commission, Supervisory Board, Commission Secretariat, specialised expert working groups, and the Special Supervisor.

[101] General Comment 16, ibid at §10.

[102] GDPR, Recital 64.

[103] GDPR, Article 16.

The Data Protection Commission is designated to oversee the Act. The Commission is formed by the ICT Minister as head of the Commission, with additional members: the Intelligence Minister, the Interior Minister, the Justice Minister, the Culture Minister, the Finance Minister, the Secretary of High Council for Cyberspace, the head of the National Center for Cyberspace, the deputy head of the Judiciary in charge of the Prevention Department, the Head of the Article 90 Committee of the Majlis (Parliament), the National Prosecutor, and the Secretary of the Information Technology executive council as the Commission's secretary.

Powers for the Commission are set out in Articles 41 and 42. The Commission is given powers to regulate and supervise the expert working groups that are also in charge of overseeing the Act and more generally, to coordinate the organs in charge of the implementation. The working groups determine the regulatory and supervisory affairs.

The Supervisory Board will supervise how well the supervisory tasks of expert working groups are being fulfilled and will receive complaints from stakeholders in personal data safeguarding and following up on them. This is clearly a function for the Commission staff to be handling rather than any oversight body.

A Special Supervisor will be appointed pursuant to Article 54 for the processing of vital and sensitive personal data, grand processing of personal data, serious and numerous damages of processing of personal data, and other tasks as determined by the Supervisory Board.

According to the present Draft Act, all powers and tasks in relation to the application of the Law will be established by the Commission.

It is unclear why it is necessary to create such a complex structure while other countries have a single commission under which all activities are conducted by a secretariat and perhaps an oversight board who reviews its activities.

2. Problems of Independence in Bodies

Two issues are of concern in relation to the Commission as set out. Firstly, it is composed solely of Government ministers and other representatives of security-related State bodies. This composition clearly lacks representatives whose field of expertise pertains to human rights or consumer rights. Secondly, the Commission sits in the headquarters of the ICT Minister. This constitutes a further aspect of great concern about the independence of the oversight body.

It should also be noted that the Draft Act proposes that the Supervisory Board and the Commission have members in common such as the Minister of Justice. This aspect poses a serious threat to the independence of the oversight bodies.

International law clearly requires that the oversight body must be functionally and administratively independent from all public authorities. The 1990 Guidelines for the regulation of computerised personal data files state:

> The law of every country shall designate the authority which, in accordance with its domestic legal system, is to be responsible for supervising observance of the principles set forth above. This authority shall offer guarantees of impartiality, independence vis-a-vis persons or agencies responsible for processing and establishing data, and technical competence. [104]

More recently, the General Assembly Resolution on the Right to Privacy in the Digital Age of 19 December 2016 called on states to:

> Establish or maintain existing independent, effective, adequately resourced, and impartial judicial, administrative, and/or parliamentary domestic oversight mechanisms capable of ensuring transparency, as appropriate, and accountability for State surveillance of communications, their interception, and the collection of personal data.[105]

[104] Guidelines for the Regulation of Computerized Personal Data Files, G.A. res. 45/95, 14 December 1990, paragraph 8.

[105] The right to privacy in the digital age, G.A. res. 71/199, 19 December 2016

The EU General Data Protection Regulation (GDPR) requires each Member State to set up oversight authorities which "act with complete independence in performing its tasks and exercising its powers in accordance with this Regulation".[106] The GDPR further requires Member States to "provide for each member of their supervisory authorities to be appointed by means of a transparent procedure by: — their parliament; — their government; — their head of State; or — an independent body entrusted with the appointment under Member State law".[107]

In a recent case at the Court of Justice of the European Union, the Court noted that "the supervisory authorities whose task it is to supervise the application, in the territory of their own Member States, of the provisions adopted by those States pursuant to the directive are to act with complete independence in exercising the functions entrusted to them".[108] The Court further held that:

> The guarantee of the independence of national supervisory authorities is intended to ensure the effectiveness and reliability of the monitoring of compliance with the provisions concerning protection of individuals with regard to the processing of personal data and must be interpreted in the light of that aim. It was established in order to strengthen the protection of individuals and bodies affected by the decisions of those authorities. The establishment in Member States of independent supervisory authorities is therefore, as stated in recital 62 in the preamble to Directive 95/46, an essential component of the protection of individuals with regard to the processing of personal data.[109]

Similarly, Modernised Council of Europe Convention 108 states that "The supervisory authorities shall act with complete independence and impartiality in performing their duties and exercising their powers and in doing so shall neither seek nor accept instructions"[110] and "shall deal with requests and complaints lodged by data subjects concerning their data protection rights and shall keep data subjects informed of progress".[111] In its modernisation process, the effective enforcement of data protection rules by independent supervisory authorities in the Contracting Parties is considered central to the Convention 108's practical implementation. To this end, the Modernised Convention underlines the need for supervisory authorities to be vested with effective powers and functions and to enjoy genuine independence when fulfilling their mission.[112]

The proposed Iranian system is also less independent than many of its regional neighbours. In comparison, the Data Protection Authority in Bahrain was tasked to receive individual complaints concerning violation of the data protection law, examining them and determining their seriousness.[113] A right to appeal has been introduced by way of a judicial committee established in the Commission (called the Appeals Committee), which shall be competent to adjudicate appeals submitted to it.[114]

In Algeria, the Data Protection Authority is formed by members elected by the President of the Republic, the judicial branch, the Parliament, the National Commission for Human Rights, as well as representatives of the Ministries of defence, foreign affairs, interior, justice, communication, health, and labour.[115] Tunisia, the Organic Act on the Protection of Personal Data created the "Instance Nationale de Protection des Données à Caractère Personnel" as an autonomous legal entity with an independent budget established by the Ministry of Human Rights.[116]

---

[106] GDPR, Art. 52 (1).

[107] GDPR, Art. 53 (1).

[108] Case C-210/16 Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v Wirtschaftsakademie Schleswig-Holstein GmbH (Wirtschaftsakademie case), 5 June 2018, p 68.

[109] Case C-362/14, Maximillian Schrems v Data Protection Commissioner, 6 October 2015, p 41.

[110] Council of Europe, Modernised Convention for the Protection of Individuals with Regard to the Processing of Personal Data, Amending protocol to the Convention for the Protection of Individuals with Regard to the Processing of Personal Data, Article 15(5).

[111] Article 15 (4).

[112] Handbook on European Data Protection Law, 2018 edition https://fra.europa.eu/en/publication/2018/handbook-european-data-protection-law.

[113] Bahrain Law No. (30) for the year 2018 Issuing the Personal Data Protection Act, Art. 30.

[114] Bahrain Law No. 30, Art. 34.

[115] Algeria Law on the Protection of physical persons for the processing of personal data, 10 June 2018, Art. 23.

[116] Tunisia Organic Act 2004-63 on the Protection of Personal Data, 27 July 2004, Art. 75.

Recommendations

- Streamline the structure of oversight bodies to ensure the independence of the Commission. This should be an independent regulatory body for the protection of personal data, which is politically, administratively, and financially independent from any public authority and is given adequate resources to conduct its activities with members elected by the parliament, the judiciary, the government, as well as from the private sector.

F. Lack of Adequate Remedies

Another significant problem is the lack of enforceable remedies provided for in the law available to individuals when their privacy rights are violated.

Article 72 of the Draft Act sets out seven "enforcement measures that are ratifiable by the Commission and "suggestible by expert working groups". These include: financial penalty, ban from activity or service in one or more professional ranks for a set period, ban from activity or service in all or some governmental bodies or corporations for a set period, and reducing the length of license.

Article 53 on the tasks of the Supervisory Board, states that it receives "complaints from data subjects personal data safeguarding (Act)" and too generally provides that it will "follow up on them".

The Draft Act does not present any remedy for individuals to appeal against such decisions before superior or judicial bodies.

According to international standards, adopting legal instruments is not sufficient to ensure the protection of personal data. To make data protection rules effective, it is necessary to establish mechanisms that enable individuals to counter violations of their rights and to seek compensation for any damage suffered. It is also important that supervisory authorities have the power to impose sanctions that are effective, dissuasive, and proportionate to the infringement in question.

The importance of having effective remedies is stressed by General Comment 16 as follows:

> Provision must also be made for everyone effectively to be able to protect himself against any unlawful attacks that do occur and to have an effective remedy against those responsible.[117]

In the European region, both the CoE and the European Union law grants to individuals the right to lodge requests and complaints to the competent supervisory authority if they consider that the processing of their personal data is not being carried out in accordance with the law.

The Modernised Convention 108 recognises the right of data subjects to benefit from the assistance of a supervisory authority, irrespective of their nationality or residence. A request for assistance may only be rejected in exceptional circumstances, and data subjects should not cover the costs and fees related to assistance. The Conventions in particular states that data subjects have a right to:

> Have a remedy under Article 12 where his or her rights under this Convention have been violated.[118]

Article 12 provides that each party to the Convention:

> Undertakes to establish appropriate judicial and non-judicial sanctions and remedies for violations of the provisions of this Convention.[119]

[117] General Comment 16, ibid at §11.

[118] Council of Europe, Modernised Convention 108, Art. 9.

[119] Council of Europe, Modernised Convention 108, Art. 12.

The Explanatory Report further stresses the importance of ensuring remedies to data subjects as a way to ensuring effective implementation:

> The effectiveness of the application of the measures giving effect to the provisions of the Convention is of crucial importance. The role of the supervisory authority (or authorities), together with any remedies that are available to data subjects, should be considered in the overall assessment of the effectiveness of a Party's implementation of the Convention's provisions.[120]

The same principles are enshrined in the GDPR that require supervisory authorities to adopt measures to facilitate the submission of complaints. They must be investigated, and the supervisory authority must inform the person concerned of the outcome of the proceedings dealing with the claim. The GDPR requires Member States to grant data subjects a judicial appeal against decisions by a national authority. This applies not only to data subjects but also to controllers and processors that have been party to the proceedings before a supervisory authority.[121]

This right of appeal is widely accepted and implemented internationally and other countries in the region have given data subjects the right to effective remedies together with the possibility of a judicial appeal. The Tunisian data protection law states that the data protection authority ("Instance Nationale de Protection des Données à Caractère Personnel") receives complaints and determines the necessary measures to ensure data protection.[122] The Law further ensures a right to judicial review of the authority's decisions before the Court of Appeal in Tunis within one month since the decision has been issued.[123] In Qatar, the Personal Data Privacy Law provides that the Competent Department may issue a reasoned decision to oblige the controller or the processor to set right the violation complained on within a specified period by the Competent Department itself. The controller or the processor are given 60 days from the notification to appeal any decision taken before the Minister. The Minister will settle any appeal within 60 days from the date of filing.[124] Similarly, in Algeria, the Data Protection Authority receives individual complaints and to order any modification it may consider necessary for the protection of personal data including to stop processing as well as the destruction of personal data. [125]

Recommendations

- Give Commission binding powers to order stopping of processing, correction, release of personal information to the subject, and other powers.
- Give individuals a remedy to appeal against the Commission's decisions before judicial bodies.

[120] Council of Europe, Modernised Convention 108, Explanatory Report, par. 35.

[121] GDPR, Arts. 57, 77 and 78.

[122] Tunisia, Organic Act 2004-63 on the Protection of Personal Data, 27 July 2004, Art. 76.

[123] Tunisia, Organic Act 2004-63 on the Protection of Personal Data, 27 July 2004, Art. 82.

[124] Qatar, Personal data Privacy Law No. 13 of 2016, Art. 26.

[125] Algeria, Law 18-07 of 10 June 2018 on the protection of physical persons in the processing of personal data, Art. 25.

V. Conclusion

The Personal Data Protection and Safeguarding Draft Act is in clear need of improvements to ensure that Iran is compliant with its international obligations on data protection and privacy, as well as to ensure compliance with the GDPR and other laws to facilitate the transborder flow of personal information.

The Draft Act is insufficient to provide those protections, and further endangers free expression and right of access to information under the Iranian constitution. It omits international standards and laws, and leaves data subjects vulnerable to problematic provisions of the Islamic Penal Code and the Computer Crimes Law. The implications of this Draft Act for freedom of expression are numerous. Most significantly, the realities of this law's enforcement of data localisation towards the centralisation of information and granting of control to Iranian authorities is concerning. Significant omissions and concerns exist about the independence of the Data Protection Commission and oversight bodies in ensuring that due process is applied. Additionally, the lack of clear remedies for violations of the rights of data subjects is a dangerous omission given the dangerous precedent set within the Iranian judiciary for persecution and harassment of individuals practicing their right to freedom of expression. The Draft Act should be sent back to the draft committee with public and expert consultations held prior to reintroduction in Parliament.

Appendix: Translation of Draft Act

Draft Act

Personal Data Protection and Safeguarding

Introduction

In implementing:

A) Various articles of the Chapter three of the Constitution of the Islamic Republic of Iran on the 'Rights of Nation,' especially articles 19, 20, 22, 23, 25, 26, 38 and 39;

B) General policies of the regime, as outlined by His Excellency the Supreme Leader on:

1- Cyber networks (especially provisions 1 and 7)

2- State administration (especially provision 23)

3- Civil defense (especially provision 11)

4- Security of the space for production and exchange of information and communications (especially provision 1)

and

5. The Sixth Development Plan (especially provision 36 and 53-3) and

C) Other laws, especially the following:

1) The Tasks and Authorities of the Ministry of Information and Communications Technology of Iran Act

2) Free Publication and Access to Information Act

3) Cyber Trade Act

4) Islamic Penal Code— the Tazirat section

5) Code of Criminal Procedure

6) Code for Punishment of individuals who commit Illegal Audiovisual Activity

7) Sixth Development Plan Act

8) Press Code

9) Aims and Duties of the Ministry of Islamic Culture and Guidance Act

10) Healthy Administration and Anti-Corruption Act

11) Registration of Patents, Industrial Designs and Trademarks Act

12) Trade Act

13) Supporting Customer Rights Act

14) Guild Organization Act

And in implementing the fatwa by the Supreme Leader that declared violation of privacy to be *Haram* the "Personal Data Protection and Safeguarding Act" is hereby ratified.

Chapter One: General

Section One: Aim of the Law

Article 1. The main aim of this law is protecting the reputation and dignity of the persons who are subject of data by the followings ways, the regulations of which are detailed below:

a) Stipulating the rights of persons who are subject of data, especially in interaction with other legitimate rights

b) Regulating private data procession

c) Accountability of data processing

d) Synergy of regulatory and supervisory matters of data processing

e) Reparations for damages and harm of data processing

Section Two: Definition

Article 2: Definition of terms:

a) **Personal data** consists of data that, on its own or together with other data, directly or indirectly, identifies the individual subject of the data by reference to an identifier.
b) **Sensitive personal data** includes personal data that reveals the tribal or ethnic roots, political, religious or philosophical opinion, hereditary details or health information of an individual.

c) **Processing** means any manual or automatic operation on private data including (but not limited to) creation, registration, reception, collection, keeping, separation, change, analysis, classifying, structuring, adapting, saving, sharing, sending, distribution and presenting, publishing and making it accessible and erasure.

d) **Controller** is an individual who determines all or part of aims, mechanism, conditions, specifications and tools of one or several processing operations on private data held by the processor. Ratifications or decisions of relevant authorities in regulation, supervision and adjudication of private data processing does not count as 'controlling,' except in cases where it pertains to individuals.

e) **Processor** is the individual who acts on behalf of the controller. If there is no controller or processing can't be attributed to him or her, the processor can also be known as controller.

f) **Special supervisor** is an individual who, following an edict issued by the commission, will have the authority to supervise processing of private data.

Section Three: Scope of application of the law

Article 3: Individuals to whom the law is applicable in this law are the following:

a) Iranian citizens: individuals or corporations, public or private, whether their private data is being processed inside or outside Iran.

b) Foreign citizens: individuals or corporations, public or private, only if their data is processed by Iranian processors or controllers.

Chapter Two: Rights of persons who are subject of data

Section One: Consent to processing

Article 4: Processing non- public personal data is conditional on the consent of person subject of data.

Article 5: Consent given by individuals subject of data should conform to the following conditions:

a) Given prior to processing

b) Express the knowledge of the individual

c) be referable

Article 6: Processing private data about public situations or states without the consent of the person or persons who are subject of data is only allowed if:

a) The person has made the data prone to processing; or

b) They not limited the processing of their data.

Article 7: Consent obtained by deception or threat or ambivalence of the person is not valid and if the person is not of capacity, the consent of his or her guardian or guarantor is necessary. State of coma or similar states which mean the person doesn't have intention or will mean that he or she lacks the legal capacity to give consent.

Section Two: Request processing or cessation of processing

Article 8: The person who is the subject of data has the right, at any time, to request processing or cessation of processing of all or part of data from controller, if the following conditions are met:

a) Data or their outcome are incorrect;

b) Data or their processing is outside his or her scope of consent.

Article 9: Request to process or cease to process personal data can be done with the aim of forgetting provided that there is no other data subjects.

Section Three: Processing

Article 10: In the following conditions, the person has the right to access their own data with the aim of processing them:

a) Doesn't include public classified information or other people's private data;

b) Referability of data is not disturbed

Section Four: anonymity in processing

Article 11. Giving consent to processing does not equal revealing the identity of the person who is the subject of data and the person has the right for their anonymity to be observed within the limits of the consent.

Note: Revealing of identity means knowledge by unauthorized individuals of name and family name of the individual who is the subject of data or allocated identifiers.

Section Five: Conflicting with the rights of other people

Article 12: In the following conditions, processing of private data within the framework of relevant laws without the consent of individual concerned is allowed:

a) It is necessary for safeguarding of the person's reputation, life or property.

b) It is necessary for safeguarding the reputation or life of another person or preventing acute financial damage to them

c) It is necessary for prevention of or responding to threats to public order, security or safety

d) it is necessary for discovery of crimes or violations or identifying of accused or implementation of judicial and law enforcement orders.

Note: Using any of the conditions above is only justified when no other option is available.

Article 13 - Beneficial use of private data without the consent of the person subject to them is only allowed if:

a) Anonymity is preserved

b) There is no customary material or spiritual damage to the person

c) It is not possible to get the person's consent.

Article 14 — If there is conflict between the rights of two or a few persons who are subjects of data, the following priorities shall be observed:

A) Damages to reputation over financial damages

B) Persons who have individual characteristic such as age or gender or social characteristic such as job, ethnicity or religion which are customarily vulnerable over other individuals

C) Lack of consent over implied consent and both of those over explicit consent of the persons who are subject of data

D) Non-public situations or circumstances over public situations or states

Chapter Three: Commitments of controllers and processors

Section One: Scope of commitments of controllers and processors

Article 15: Commitments in this chapter are the responsibility of controller unless law, agreement or contracts puts them on the processor.

Article 16: All the functions of the process of personal data processing should be based on the documented order or request of controller. Otherwise, processor will be also known as controller.

Article 17: If every function of processing has a separate controller or processor, they will only be responsible for that function.

Article 18: If there are numerous controllers or processors for each function, the assumption is that of equal responsibility unless it is proven otherwise.

Section Two: Credibility of process

Subsection One: Permissibility

Article 19: When the acquiring of consent from the person who is the subject of data is necessary, depending on the kind and degree of processing, the number of persons who are subject of data, the method of consent given by them and relevant costs, the relevant consent form should be designed and be considered as an inseparable part of the agreement to process.

Article 20. Playing a role in any of the functions of personal data processing as a job or independent career, even on a case by case or temporary basis, whether for profit or not, requires a license or certificate from relevant competent authorities.

Note: Possessing the license or certificate subject if this article doesn't exempt one from other requirements of this law, especially the necessity for acquiring consent from the persons who are subject of data and their observance is necessary.

Article 21. The controllers or processes of personal data are only exempt from the necessity outlined in Article 20 if they only process the personal data of their potential or existing customers only for the subject of their own activity.

Article 22. Any professional outsourcing of private data, in addition to observing other regulations, is required to be registered in the website of the relevant competent authority.

Section two: Supervision

Article 23. For this act, 'supervision' consists of any measures by relevant authorities to confirm the credibility, trustability, referability or requirements of foreign-based processing of personal data including interview, review, supervision, tracing, observance, in-person or online control by the following:

a) Managers, position-holders, direct data subjects or those related to the processing of personal data

b) Infrastructure, structures and hardware and software systems, whether exclusive or shared for processing of personal data

c) Documents, information or paper or digital data about and related to processing of personal data.

Article 24. Provision of all facilities and human resources necessary for proper implementation of supervision commitments is a responsibility of controller or processor.

Article 25. Agreement between controller or processor with the persons who are subject of data or others about supervision is only valid so far as it is not in contradiction with the supervisory commitments of this act.

Section Three: Trustability of processing

Subsection one: Transparency

Article 26. Controller or processor is obliged to make the following information avaliable to the persons who are subject of data:

a) the aim of processing, whether economic, social, cultural, health, welfare, legal, judicial or security

b) Kind and method of processing, whether gathering, changing, analysis, sharing, saving or erasing of data

c) Identity, nature and activity of main and subsidiary controllers or processors

d) Processing situations and states whether public or non-public

e) Sources of processing including the information banks of public or private bodies or various surveys

f) Processing's details and technical conditions especially in regards to choice of personal data of Iranian citizens which is the section of Section Five of this law

g) Licenses issued by relevant authorities

h) The level of security and safety of processing and knowledge and the accrued costs

i) The rights of persons who are subject of data to processing of their personal data and how to use them

j) Special supervisor of processing and other relevant supervisors and those following up on complaints by the the persons who are subject of data.

Note: Controller or processor is obliged to make the information available a month after receiving personal data, based on the provisions of this article.

Article 27. Informing the persons who are subject of data should be in accordance with their individual and social conditions and the facilities in their use and their level and, in addition to general and exclusive informing, should happen via documents such as “conditions and concerns of processing” so that their knowledge is assured.

Subsection Two: Non-threatability

Article 28: Each of the functions and stages of processing should enjoy their own special safety and security provisions. These should cover all the three following levels:

a) Physical security and safety including infrastructure, structures and relevant hardware systems

b) Safety and security of information including all software and hardware processors

c) Human safety and security including all main and subsidiary controllers and processors

Article 29. Required or suggested safety hardware and software processes and tools should meet the following conditions:

a) Kind and degree of damage caused by potential and active threats from the point of view of persons who are subject of data;

b) Being practical;

c) technical and executive capacity.

Article 30. The persons who are subject of data can only require the controller or processor to observe safety and security provisions above those of the regulations of relevant authorities if implication of these doesn’t disrupt their responsibilities and if they can bear the cost.

Subsection three: Accountability

Article 31. Controllers should be fully responsible to persons who are subject of data; whether their responsibilities emanates from an agreed contract or memorandum of understanding or documents like privacy guidelines.

Article 32. The assumption is that the rights of persons who are subjects of data won't be trampled upon and the controller is obliged to observe all of these rights unless the opposite can be proven.

Section Four: Referability of processing

Article 33. Controller or processor is required to safeguard all or any data and information mentioned below until at least six months after erasure of personal data:

a) Log files and traffic data obtained by processing of personal data;

b) Identity information of persons who are subjects of data;

c) Kinds of processing done to the relevant data and their aim or aims.

Note: the commission can increase the time for keeping and securing of information or data relevant to this article to two years, on a case by case basis.

Article 34: If the correctness and integrity of personal data of someone is violated, it is incumbent upon the controller or processor to keep all original and inaccurate data for six months from the date of last processing that led to the inaccuracy.

Article 35. Data and information relevant to this section can be used against controller and processor.

Article 36. If the relevant authorities issued general safeguarding regulations and instructions, implementig them in processing of personal data is necessary and the cost is to be borne by the controller or the processor.

Note 1. Implementation of private regulation and instructions of the safeguarding chain is incumbent upon bearing of the costs by the requester and it not contravening general regulations.

Note 2. Controller can ask for priority order from the commission if regulations and instructions contradict one another.

Section Four: Foreign-based processing

Article 37. In the cases below, the processing of personal data is considered foreign-based:

a) If any of the controllers or processors holds foreign citizenship

b) If the systems that process data exist outside the sovereign realm of the Islamic Republic of Iran

Article 38. For the processing of personal data of Iranian citizens, the following conditions need to be met:

a) They can only be stored in the data centers located in the sovereign realm of the Islamic Republic of Iran or the foreign-based data centers approved by the relevant authorities;

b) All hardware and software processors should hold licenses issued by relevant authorities;

c) They should be transferred on trustable communication networks;

d) Relevant authorities have to confirm the foreign controllers and processors;

e) Foreign-based processors should register based on regulations.

Chapter Four: Regulation and supervision of personal data

Article 39: Regulation and supervision of personal data is the responsibility of following organs:

a) Personal data protection commission

b) Supervisory board

c) Expert working groups

d) Executive secretariat of the commission

Section One: Personal data protection commission

Subsection One: Commission members

Article 40: Commission is to be formed of the following individuals:

1) ICT minister as head of the commission
2) Intelligence minister
3) Interior minister
4) Justice minister
5) Culture and Islamic Guidance minister
6) Economic Affairs and Finance minister
7) Secretary of Supreme Council of Cyberspace and head of the National Center for Cyberspace
8) Deputy head of the Judiciary in charge of the Prevention of Crimes Department
9) Head of the Article 90 Committee of the Majlis (parliament)
10) Attorney- General
11) Secretary of the Information Technology executive council as commission's secretary

Note 1. The meetings of the members or their deputies are held by the decision of the chair by official invitation.

Note 2. The chair of the Commission issues membership confirmations.

Subsection 2: Commission tasks and authorizations

Article 41: The commission has the followings tasks and authorizations:

a) Coordinating the regulation and supervision tasks of the expert working groups with each other and also with the supervisory board

b) Moderating, mixing or separating tasks of members of expert working groups based on their legal authorities

c) Ratifying the internal and commission secretariat's bylaws

d) Solving disputes between expert working groups and supervisory board and also those with other governmental authorities

e) Suggesting necessary strategic legislation to relevant authorities

f) Coordinating ratifications and decisions of the commission, expert working groups and supervisory board with country's administrative regulations

g) Issuing appointment orders for heads of expert working groups and special supervisors

h) Hearing the report of the supervisory board and special supervisors about the missions of the commission and deciding on them

i) Reporting to higher authorities about the status of safeguarding personal data, their regulation and monitoring of their processing

Article 42: The ratifications and decisions of the commission are binding for expert working groups and the supervisory board.

Subsection 3: Commission meetings and ratifications

Article 43: The meetings of the commission will be official only when attended by two thirds of the commission members. Its ratifications pass by majority vote.

Article 44: Members and experts of working groups and also other officials and experts can take part in commission meetings and offer their opinion, if deemed necessary by the chair of the commission.

Subsection 4: Commission Secretariat

Article 45: The commission secretariat sits in the headquarters of ICT Ministry.

Article 46: The secretary of commission is tasked with the following:

a) Taking care of secretarial affairs of the commission;

b) Coordination and supervising of executive secretariats of the expert working groups and the supervisory board;

c) Communication and publication of commission ratifications and decisions;

d) Holding meetings and suggesting their agenda, inviting members and others to take part and other related affairs;

e) Suggesting executive by-laws for the secretariat to be passed by the commission.

Section 1: Expert working groups for safeguarding personal data

Subsection 1: Forming working groups

Article 47. Expert working groups consist of representatives of bodies in charge of governmental affairs in relation to safeguarding of personal data who are concerned with the tasks outlined in this act.

Article 48. In the first meeting of the commission, the by-laws for formation of working groups including sections and their scope of work, chair, secretary and location of the secretariat, tasks and missions, procedure for administration and officiating meetings and ratifications, interaction with working groups, reporting to the commission and other relevant authorities will be ratified.

Subsection 2: Working group tasks and authorizations

Article 49. Bylaws for formation procedure and doling out the tasks and authorizations of expert working groups will be adopted by the commission within three months and then ratified by the Cabinet.

Article 50. The regulations determined by the expert working groups in each of the regulatory and supervisory affairs will be binding after the commission's approval and ratification.

Section 3: Board of Supervision over personal data (Supervisory Board)

Subsection 1: Members of Supervisory board

Article 51: Supervisory Board will have the following as members:

1. Justice minister as head of the board
2. Head of the Article 90 Commitee of Majlis
3. Head of the National Centre for Cyberspace
4. Secretary of Commission

Article 52. The Supervisory Board is to meet in the headquarters of the Justice Ministry. The by-laws for formation and working procedure of the board and its secretariat is to be ratified by the commission.

Subsection 2: Tasks of the Supervisory Board

Article 53. The Supervisory Board is tasked with:

a) Supervising how well the supervisory tasks of expert working groups are being fulfilled;

b) Receiving complaints from data subjects of personal data safeguarding (Act) and following up on them;

c) Identifying special supervisors and introducing them to the commission and supervising their affairs and activities based on the manual passed by the commission;

d) Supervising drafting of expert manuals on referability of evidence pertaining to personal data by expert working groups, ratification in commission and their publication after approval by the commission head;

e) Other tasks as determined by the commission.

Subsection 3: Special supervisor

Article 54. For the following tasks, a special supervisor will be appointed:

a) Processing of vital and sensitive personal data

b) Grand processing of personal data

c) Serious or numerous damages, potential or active, of processing personal data;

d) Other tasks as determined by the Supervisory Board and approved by the commission.

Article 55. Special supervisor should meet the following criteria:

a) Lack of criminal or police record;

b) Having a good reputation;

c) Having necessary skills and expertise;

d) Not having conflict of interest with the subject of supervision.

Article 56. The length of mandate for the special supervisor will be determined in two ways:

a) Case by case, based on the subject allocated;

b) For a period of three years and extendable for a similar length of time.

Article 57. Conditions for the activity of the special supervisor consist of:

a) His tasks and missions up on the suggestion by the Supervisory Board, ratified by the commission and delivered to him;

b) Scope of the work of the special supervisor has to be specifically defined and vague and expansive supervisory matters are not considered credible;

c) Controllers and processors must bear the cost of regular supervisory needs of the special supervisor;

d) Supervisory board is tasked to provide legal support and the necessary facilities for the special supervisor to be able to conduct his or her tasks the best;

e) The special supervisor is personally responsible for the work and is not entitled to contract out all or some parts of it;

f) Cessation or suspending the activities of him or her, his or her dismissal or accepting his or her resignation are only possible by the commission;

g) During his or her period of assignment, the special supervisor doesn't have the right to accept supervisory tasks outside the framework outlined by the commission, whether for profit or otherwise.

Section 4: Budget for regulation and supervision of personal data

Article 58. The budget necessary for this law will be outlined centrally as part of the commission secretariat budget and will have an independent column in budget laws.

Section 5: Responsibilities and enforcement guarantees

Subsection 1: scope of responsibility for controllers and processors

Article 59. Controller and processor are independently responsible for their commitments.

Article 60. The processor is only exempt from responsibility if:

a) His task is not in contradiction with the order or request of the controller;

b) If the order or request is considered illegal, the controller has been made aware; and

Section 2: Civil responsibilities

Article 61. The controller up on the request of the person affected by the damage is responsible to provide reparation for the person subject of data. If this is not done, the person affected by the damage can follow up via judicial authorities.

Subsection 1: Material reimbursement

Article 62. When an individual associated with a corporation brings damage to someone, it is the corporation that will be responsible for the cost. Unless the corporation is able to prove that the individual acted outside his or her authority and that the corporation didn't fail to supervise how well he or she was doing the job.

Article 63. If the person who is subject of data gets his/her rights unjustly and brings damage to another person, he or she will be responsible.

Article 64. Based on the kind and extent of the damage brought to reputation, the amount of damage or the financial cost brought by it, relevant judicial or law enforcement authorities can require the party who has brought the damage to pay financial penalty or accept social limitations. The manual to determine financial cost incurred by illicit processing of personal data and to show ways in which a reputation damaged by spiritual hurt can be restored and what penalties can be impressed will be suggested by expert working groups and ratified by the commission.

Section 3: Penal responsibilities

Subsection 1: Crimes and penalties

Article 65. The penalty deemed out in this law will only be implemented if other law doesn't stipulate a heavier punishment for these crimes.

Article 66. Any reference to data that has resulted from violating the regulations of this law is illegal and will be punished with fifth degree sentences.

Article 67. Any of the functions of processing for which other law stipulates criminal charge and punishment will be treated according to those laws.

Article 68. Those who have committed the following will be punished accordingly:

a) Violating the right of consent of persons who are subject of data, if the data of non-public situations and states is processed, will bring out fifth degree punishment and if data of public situations and states are processed, sixth degree punishment;

b) Preventing fulfillment of all or part of the right to request from the person who is subject of data about processing or its cessation or self-processing or violation of right to anonymity — One or both counts of sixth degree punishment;
c) Violation of commitments to credibility, trustability or referability of processing personal data — One or both counts of fifth degree punishment;
d) Illicit use of the laws stipulated in this law by the person who is subject of data, based on the amount of damages incurred — One or both counts of sixth degree punishment;
e) Illicit control by the relevant authority in the government will lead not only to the stipulated punishment for the said crime but six to three years of ban from government service;
f) Not implementing or incorrect implementation so that all or some of the regulations of this act or orders of the commission or the supervisory board or special supervisor is not followed (like by not keeping all or part of data) — One or both counts of fifth degree punishment.

Note 1. The court can urge the violator to pass special classes on safeguarding personal data and receive relevant licenses, as stipulated by the manual passed by the commission.

Note 2. If the corporations who are subject of the Article 747 of the Islamic Penal Code commit the crimes outlined in Articles 69, 70 and 71 of this act, they will be punished according to the Article 748 of this act.

Subsection 2: Aggravation of punishment

Article 69. If one or more of the conditions below are met, the punishment will be increased with one or two degrees:

a) If the crime has been committed in association with one's job or career;

b) If in relation to the scope of one's activity, large number of individuals have been targeted;

c) Financial cost or spiritual damage is considerable or unrepairable;

d) Vital or sensitive personal data are tools or results of crime; and

e) They are committed as a group or in an organized manner.

Article 70. If the financial benefits gained by committing of these crimes are more than the financial penalty stipulated for them, the former will be considered. If a prison sentence is imposed in lieu of financial punishment, the difference between the financial benefit mentioned in this article should be also given out as financial punishment.

Section 4: Disciplinary responsibilities

Subsection 1: Disciplinary breaches

Article 71: The suggested disciplinary breaches by expert working groups, to be passed in the commission, include the following:

A) All crimes stipulated in this law;

B) Violation of commitments of controller and processors, including credibility, trustability, referability and foreign-based processing;

C) Violation of commitments of persons who are subject of data toward other stakeholders;

D) Violation of contractual commitments or those stipulated in other binding documents.

Subsection 2: Disciplinary enforcement measures

Article 72. Disciplinary enforcement measures, ratifiable by the commission and suggestible by expert working groups, in accordance with prevention standards, proportionality and effectuality can include any of the following:

a) Financial penalty;

b) Ban from activity or service in one or more professional ranks for a set period;

c) Ban from activity or service in all or some governmental bodies or corporations who are subject of this law for a set period;

d) Reducing the length of license or seniority or its suspension for a set period;

e) Ban from extension of license or contract or receiving of license or contact or gaining other positions for a set period;

f) Repealing license or contract or ban from service for a set period.

Note 1. Expert working groups are tasked with classifying their disciplinary enforcement measures contracts based on the regulations of the Islamic Penal Code.

Note 2. Adjudicating the conditions of violation and issues related to aiding, abetting, participation, repeating, responsibility of violating corporations and the like and factors that exempt, reduce of aggravate responsibility are those stipulated in the Islamic Penal Code.

Section 5: Guarantee of contractual enforcement

Article 73. Any agreement that contradicts the provisions and necessary regulations of this law is not credible and will be thus nullified.

Article 74. Parties to agreements subject to this law are required to consider violations and crimes stipulated in it as violation of agreement and stipulate contractual enforcement that is proportional, effective and preventive.

Section 6: Preventing violations and crimes

Article 75. Responsibility of drafting prevention programs is with the expert working groups which will be approved by the commission.

Section 7: Statistics and information

Article 76: Any of the professional working groups is tasked with making statistics and information on civil, penal, police and contractual information of their own section available and up-to-date based on the by-laws passed by the commission.

Chapter 6: Repeal of laws and devising of necessary regulations

Article 77: From the date of ratification of this act, all laws and regulations in contradiction with this will be repealed. This law, so long as it has not been replaced by future law or its provisions are not explicitly reformed (by legislation that names the act specifically) will remain in force.

Article 78. The executive by-laws for this act will be drafted by the members of the commission, three months after its formation, and will be submitted to the cabinet for ratification.