How to ensure digital privacy for all?

United Nations Human Rights Council (UNHRC)

By PÉRIEL Noah and CURRY Xavier

CONTENTS

INTRODUCTION TO THE COMMITTEE

UNHRC FLAG: UNHRC website

The UN human rights programme started as a small division at UN Headquarters in the 1940s. In line with that programme, the office of the United Nations High Commissioner for Refugees (UNHCR) was created in 1950, during the aftermath of the Second World War, to help millions of Europeans who had fled or lost their homes. The division later moved to Geneva and was upgraded to the Centre for Human Rights in the 1980s. The **Vienna Declaration and Programme of Action**, adopted at the World Conference on Human Rights (14-25 June 1993), made concrete recommendations for strengthening and harmonizing the UN's human rights monitoring capacity. Over time, a number of UN human rights bodies have been established to respond to evolving human rights challenges. These bodies include the Human Rights Council and its thematic and country mandated independent experts.

The United Nations Human Rights Council (UNHRC) is an intergovernmental body within the United Nations (UN) system, responsible for strengthening the promotion and protection of human rights around the globe, such as the freedom of belief and religion, the rights of ethnic minorities and indigenous people, the rights of LGBTQ+ communities, and more generally democracy, welfare, and social justice.

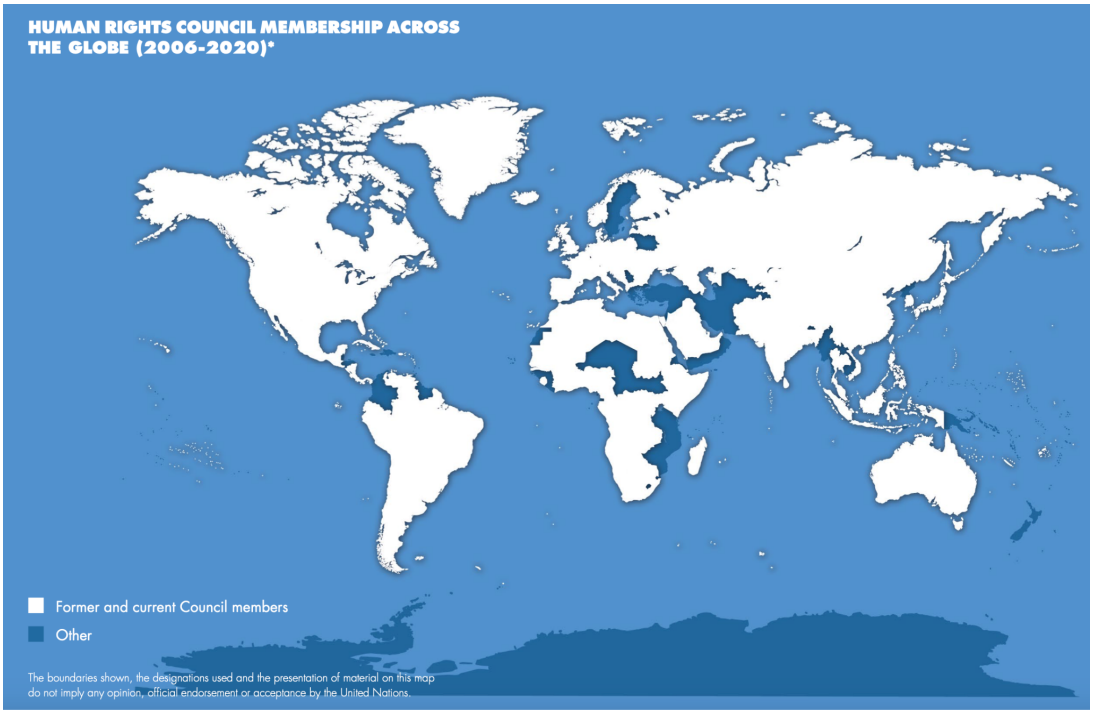
The Council holds meetings throughout the year providing a multilateral forum to address human rights violations wherever and whenever they occur. It responds to human rights emergencies and makes recommendations on how to defend, preserve and better implement human rights on the ground. The Council has the ability to discuss all thematic human rights issues and country-specific situations that require its attention.

The Council held its first session in June 2006. One year later, the Council adopted its “Institution-Building” package by resolution 5/1 to guide its work and set up its procedures and mechanisms. Among the Council’s subsidiary bodies are the Universal Periodic Review

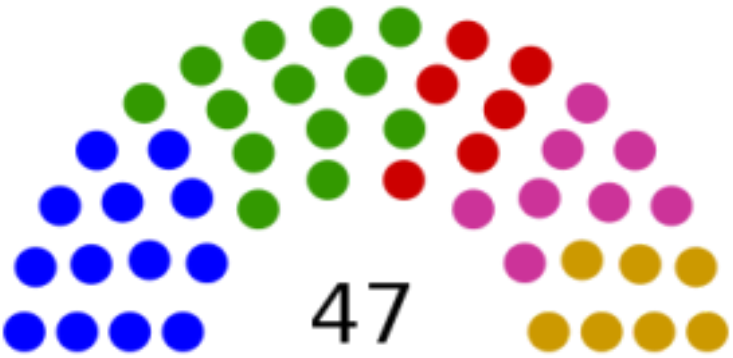
mechanism (UPR), the Special Procedures, the Advisory Committee and the Complaint Procedure.

The Council is made up of 47 member States who are elected by the UN General Assembly by a simple majority vote. They are elected for three-year terms with one-third of the members being renewed each year. Council membership is based on equitable geographical distribution of seats according to the following regional breakdown: 13 African States; 13 Asia-Pacific States; 8 Latin American and Caribbean States; 7 Western European and other States; 6 Eastern European States. 117 countries have served as Council members so far, reflecting the UN's diversity giving it legitimacy when speaking out on human rights violations in all countries.

The Council can also establish international commissions of inquiry and fact-finding missions investigating and responding to human rights violations, to help expose violators and bring them to justice.



CURRENT MEMBERS OF THE UNHRC (extracted from OHCHR website)



CURRENT COMPOSITION OF THE UNHRC

13 African States : Algeria, Benin, Cameroon, Côte d'Ivoire, Eritrea, Gabon, Gambia, Malawi, Morocco, Senegal, Somalia, South Africa, Sudan

13 Asia-Pacific States : Bangladesh, China, India, Kazakhstan, Kyrgyzstan, Malaysia, Maldives, Nepal, Pakistan, Qatar, United Arab Emirates, Uzbekistan, Viet Nam

6 Eastern European States : Czechia, Georgia, Lithuania, Montenegro, Romania, Ukraine

8 Latin American and Caribbean States : Argentina, Bolivia, Chile, Costa Rica, Cuba, Honduras, Mexico, Paraguay

7 Western European and Other States : Belgium, Finland, France, Germany, Luxembourg, United Kingdom of Great Britain and Northern Ireland, United States of America

---

INTRODUCTION TO THE SUBJECT

Over the last few decades, the world has faced **unprecedented and extraordinary innovations, namely the internet**. Since its creation in the early 1980s, the internet has grown massively popular, especially since the last fifteen to twenty years. While at the time of its launch the internet was very niche and difficult to use, today it is an important element of our daily lives. Most of the things we do are closely linked to it - from communication, researching information, reading, to entertainment. Nearly 60% (approximately 5 billion people) of the global population uses the internet as of 2020; there were only 3 million users worldwide in 1990, which means there are now 1 700 times more users today than what there were 20 years ago !

As a consequence, the number of **electronic devices** - whether they be smartphones, tablets or computers - has also massively increased. According to the Radicati Group, a technology market research firm, there were nearly 16 billion mobile devices in operation in the world in 2022. An overwhelming majority of the population, whether it be young or elderly, uses one. More specifically, in 2020, 62% of the world population had a smartphone; only 0,25% in 1990.

The multiplication of internet users and device owners brings enormous **challenges**, environmental, ethical, societal, but most interesting for us : human rights, especially privacy and protection of users' data.

There are different ways to tackle the issue of privacy. First, there is a distinction to make between **data protection and data privacy**. Data privacy defines who has access to data, meanwhile data protection is what ensures data privacy. It is the tools and policies that restrict access to the data from unauthorized sources. Data privacy and protection are two key terms generally applied to personal health information (PHI) and personally identifiable information (PII) (e.g. name, address, social security number or other identifying number or code, telephone number, email address, etc.).

Secondly, both **the user and the authorities/companies play a vital role** in data privacy and protection. The user can favor some practices to preserve his data, like only using trusted websites, using strong passwords, and many more other things. The authorities/companies play a role in making sure that the data of their users is stored securely, and that data is not sold for commercial practices (although in reality, it is exactly

what they do). Data is an asset of an individual or a company. All companies have data that includes personnel's files, customer information, product details and management, trade secrets, etc., and decisions are made based on these data available. Protecting personal data mitigates risks of costly incidents, reputational harm, regulatory penalties, and other harms. It also builds trust among its customers. If a company fails to protect its data, a third person can gain access and use it for its own benefit. The company may incur loss due to a breach of data privacy and it may affect its goodwill or brand value as well. Data protection is important for an individual for the prevention of phishing scams, identity theft, and misuse of data by a third party. Therefore, data protection is important to ensure that a person's rights and freedom are not violated, ensuring fair and consumer-friendly commerce and provision of services, and preventing any harmful or life-threatening situation that may arise for not compiling the personal data protection regulation. In Europe, there are regulations which favor the users to allow their protection, which we will develop later.

But nowadays, there is an even bigger challenge ahead of us than to protect data : **artificial intelligence** (AI). It introduces new threats to our world : it will destroy thousands, maybe millions of jobs in the next few decades; the environmental cost is huge and often overlooked; and what interests us most here : human rights, privacy. We will study the case of China in the discussion of the topic to expose this issue. AI is a brand new opportunity and extremely powerful tool for authoritarian regimes like China to control its population further.

To these unprecedented challenges, we can ask ourselves : how to ensure cybersecurity and privacy for all ?

DEFINITIONS

Artificial intelligence (AI): a particular computer system or machine that has some of the qualities that the human brain has, such as the ability to interpret and produce language in a way that seems human, recognize or create images, solve problems, and learn from data supplied to it: (source)

Blacklist: a list of people, countries, etc. who are considered by a particular authority or group to be unacceptable and who should be avoided and not trusted (source)

Autocratic: demanding that people obey completely, without asking or caring about anyone else's opinions (source)

CCTV: abbreviation for closed-circuit television : a system that sends television signals to a limited number of screens, and is often used in shops and public places to prevent crime (source)

Data breach: an occasion when private information can be seen by people who should not be able to see it. (source)

Data subject: data subject refers to any individual person who can be identified, directly or indirectly, via an identifier such as a name, an ID number, location data, or via factors specific to the person's physical, physiological, genetic, mental, economic, cultural or social identity. (source)

HRI: abbreviation for Humans Rights Index : a repository of recommendations and observations issued by bodies of the United Nations human rights monitoring system (source)

TIMELINE

Date	Event
1940s	The UN human rights programme started as a small division at UN Headquarters.
1950	Publication of Alan Turing's work : "Computing Machinery and Intelligence"
1980s	The division later moved to Geneva and was upgraded to the Centre for Human Rights.
1990	0,25% of the world population owns a mobile phone. 3 million people worldwide use the internet.
April 30th 1993	The World Wide Web launched into the public domain. The web made it simple for anyone to navigate the internet.
June 14th-25th 1993	The **Vienna Declaration and Programme of Action**, adopted at the World Conference on Human Rights made concrete recommendations for strengthening and harmonizing the UN's human rights monitoring capacity. The document called for the establishment of a High Commissioner for Human Rights by the General Assembly.
1995	European Data Protection Directive.
1990s	PBoC (Popular Bank of China) begins providing corporate credit data to commercial banks.
1999	The Institute of World Economics and Politics of the Chinese Academy of Sciences is directed by Premier Zhu Rongji to recommend a system for reversing corruption in the market economy. The report, The National Credit Management System, outlines a nationwide central system to collect data on compliance, debt default, and breaches of contract. Regional pilot programs begin to establish credit ratings for individuals and corporations.

2004	Premier Jiang Zemin advocates for a social credit system at the 16th Communist Party Congress. 23 commercial and state-owned banks create a trial consumer credit database.
March 15th 2006	The Human Rights Council replaces the Commission on Human Rights by UN General Assembly resolution.
June 18th-30th 2006	The Council holds its first session in Geneva.
2006	Banks are required to report consumer credit information to The Credit Reference Center, a new independent national credit reporting agency.
2007	The Central Guidance Commission on Building Spiritual Civilization (a body that directed to build a "socialist harmonious society"), the Central Commission for Discipline Inspection (the nationwide anti-corruption organization), the Supreme People's Court, the Ministry of Finance, the Ministry of Public Security, and the State Administration for Industry and Commerce participate in the Joint Inter-ministerial Conference on Social Credit System Construction to lay the groundwork for the SCS.
January 25th 2012	The proposal for the GDPR (General Data Protection Regulation) was released.
2013	The "blacklist" of debt defaulters is created by the Supreme People's Court. The list tracks and publishes the identity of companies and individuals currently in default. It also provides for punitive actions such as travel and spending restrictions for those on the list. The Rongcheng SCS pilot program starts.
2013	The "blacklist" of debt defaulters is created by the Supreme People's Court. The list tracks and publishes the identity of companies and individuals currently in default. It also provides for punitive actions such as travel and spending restrictions for those on the list. The Rongcheng SCS pilot program starts.
2014	*The Planning Outline for the Construction of a Social Credit System (2014 - 2020)* is released by the State Council. This serves as the framework for the development of the SCS following the conclusions of the Joint Conference in 2007. The document addresses the need to build trustworthiness, integrity, and "creditworthiness" among businesses, government bodies, social organizations, and individuals. The draft law, Social Credit Construction Law of the People's Republic of China, sets the legal basis for

	the SCS.
2016	The State Councils discuss the "personal integrity score management system" and push for the standardization of blacklists.
April 14th 2016	The European Parliament and Council of the European Union adopts the GDPR.
May 24th 2016	The GDPR officially entered into force, 20 days after its publication in the *Official Journal of the European Union*.
2017	Trial SCS systems begin in 12 cities.
May 25th 2018	GDPR put into effect in member-states of the EU. It is from now on compulsory to comply with it.
July 20th 2018	The GDPR became valid in the EEA countries after the EEA Joint Committee agreed to follow the regulation.
2019	The State Council pushes for greater mechanisms for credit repair, data collection, privacy protection, and use of technology such as AI and big data to create warnings of risky behavior.
2020	62% of the world population owns a mobile phone. 60% of the world population uses the internet (approx. 5 Billion people).
April 2021	The EU AI Act is proposed by the European Commission.
June 2023	MEPs start negotiations on the final form of the AI Act.

HISTORY OF THE TOPIC

For our demonstration, the main case study is China's Social Credit System.

The idea of tying social status to good behavior as proven by a centralized ratings system originated in the ancient world; imperial China developed a system of testing officials on knowledge of Confucian classical literature, many of which dealt with good moral behavior as the foundation of a strong state. Behavioral tracking systems have been established for decades in modern China; the Hukou system registered households and individuals, and tracks and controls citizen's movements within China. It also assists in benefits administration through regional and city government programs.

The birth of the SCS system however started during the mid-1990s, with the construction of the first credit databases. The PBoC developed an early database providing

financial credit information to commercial banks. This was formalized in the 'Banking Credit Registration and Reference System' established in 1997.

In 1999, the idea surfaced. The then Prime Minister Zhu Rongji assigned a research team at the Institute of World Economics and Politics of the Chinese Academy of Sciences to investigate solutions to corrupt market behavior. In response, The National Credit Management System was released, advocating a centralized system, bringing together data from across China. The focus of the system at this stage was economic: debt default, contractual breach, and regulatory non-compliance were to be the key data for the system. From this point on, embryonic pilot testing of the system began. For example, in 2000, Shanghai introduced a credit system which assessed eligibility for loans by individuals based on payment of utility bills.

Later on, in 2004, President Jiang Zemin endorsed the social credit system at the 16th CPC party congress in his report 'Build a Well-off Society in an All-Round Way and Create a New Situation in Building Socialism with Chinese Characteristics'. The stated goal was to establish a social credit system compatible with a modern market system. In addition, trials on a consumer credit reporting database began with 23 state-owned and commercial banks across seven municipalities.

In 2006, the Credit Reference Centre was established. The Credit Reference Centre was created to be a nation-wide, independent, credit reporting agency. Banks were required to start reporting on customer creditworthiness. Through collaboration with government departments and the Supreme People's Court, additional information relevant for creditworthiness began to be reported.

One year later, in 2007, the Joint Inter-ministerial Conference on Social Credit System Construction was set up to coordinate the development of the system. Participants include key government departments and agencies such as the Ministry of Finance, the State Administration for Industry and Commerce, and the Ministry of Public Security. But members were also included from the Central Commission for Discipline Inspection (the chief anti-corruption body in China), the Central Guidance Commission on Building Spiritual Civilization (the chief ideological body in China, aimed at a "socialist harmonious society"), and the Supreme People's Court. This wide membership beyond traditional government departments is perhaps indicative of the all-encompassing nature of the planned social credit system, and the move from a focus on financial creditworthiness, to broader conceptions of trust.

In 2009, real testing of the system began. One of the most well-cited cases was the system introduced in Suining county, Jiangsu province. Individuals were given 1000 points, with the ability to gain or lose points based on their behavior. Convictions or debt non-repayment, for example, meant point deductions. These points were then used to create a letter grade from A to D. And the result of those letter grades affected employment opportunities, access to business licenses, and eligibility for government support. A more recent example is the 'Social Credit Card', introduced in Nanjing in 2016. This offers select benefits to individuals with a high social credit score, including discounts and preferential treatment by financial institutions. Assessment criteria include such considerations as the individual's willingness to donate blood, and whether the individual is recognised as a "hard worker".

The year 2013 also marked an important step in the building of the Social Credit System. The Supreme People's Court blacklist was established. This list publishes the names and ID numbers of defaulters. As well as the 'shame' associated with being on the list, defaulters were prevented from a range of 'high-end' benefits, including traveling and staying in certain hotels. In 2017, it was estimated that 8.8 million debtors had been added to this list.

The next year, a planning and coordination document was released, under the title of "Planning Outline for the Construction of a Social Credit System (2014-2020)". This document is a culmination of the work of the joint conference, and has guided the social credit system in its development for the six following years. Five objectives for the system listed in that document included establishing necessary laws and regulations for social credit, the completion of a credit investigation and sharing system for all of China, developing credit supervision systems, a market for credit services, and establishing mechanisms for keeping trust and punishing those who fail to do so.

2016 saw the State Council emphasize the standardization of blacklists and redlists. From this point, blacklists and redlists became ubiquitous (very present) across government departments, with more than 50 in operation.

The years 2017-2018 saw the widespread adoption of regional trials of the social credit system, with 12 such cities in 2017 being classified as 'model cities'. Perhaps the most prominent example is Rongchen. The city introduced a comprehensive grading and reward and punishment system. The platform involves collaboration between 142 government departments. Hundreds of positive and negative factors go into the final score, with positive scoring individuals having priority access for finance and licenses.

In 2019, the State Council released 'Guiding Opinions on Accelerating the Construction of a Social Credit System and Building a New Credit-based Supervisory Mechanism'. This directive emphasized the need for big data and artificial intelligence to provide early warning of risky actors in need of extra regulatory attention.

As for the European Union, they are very favorable to AI accompanied by regulations. In April 2021, the European Commission proposed the first EU regulatory framework for AI. It says that AI systems that can be used in different applications are analyzed and classified according to the risk they pose to users. The different risk levels will mean more or less regulation. Once approved, these will be the world's first rules on AI.

On 14 June 2023, MEPs adopted "Parliaments negotiating position on the AI Act. The talks began with EU countries in the Council on the final form of the law. The aim is to reach an agreement by the end of this year.

These restrictions are in the pathway of an existing plan called the General Data Protection Regulation (GDPR). It was originally proposed in 2012, then followed a series of negotiations between the European Commission, European Parliament (with the European Parliament Committee on Civil Liberties, Justice and Home Affairs - LIBE), and the European Council. It was adopted by parliament in May 2016, and since 2018 it is compulsory for

businesses to comply with it. Its key purpose is to protect user's personal data on the internet.

Historically, the right to privacy is part of the 1950 **European Convention on Human Rights**, which states: "Everyone has the right to respect for his private and family life, his home and his correspondence." From this basis, the European Union has sought to ensure the protection of this right through legislation. As technology progressed and the Internet was invented, the EU recognized the need for modern protections. So in 1995 it passed the European Data Protection Directive, establishing minimum data privacy and security standards, upon which each member state based its own implementing law. In 2011, Europe's data protection authority declared the EU needed "a comprehensive approach on personal data protection" and work began to update the 1995 directive. From there emerged the GDPR.

DISCUSSION OF THE TOPIC

"Autocratic governments would like to be able to predict the whereabouts, thoughts, and behaviors of citizens. And AI is fundamentally a technology for prediction."

— David Yang, associate professor of economics at Harvard

Since the last few years, the Chinese government -with the Chinese Communist Party- has been implementing what they call the "Social Credit System". The China social credit system is a broad regulatory framework intended to report on the 'trustworthiness' of individuals, corporations, and governmental entities across China.

2022 marks a new phase in the development and implementation of China's social credit system (sometimes known as 'SoCS', or the 'SCS'). Up until now, development has been guided by a national policy document known as the 'Planning Outline for the Construction of a Social Credit System (2014-2020)'. This has seen the deployment of the social credit system widely throughout China, with an estimated 80 percent of provinces, regions and cities having introduced some version of the system, or being about to do so. The implementation of the system for corporations, known as the 'corporate social credit rating' is especially advanced: more than 33 million businesses in China have already been given a score under some version of the corporate social credit system. As of June 2022, it is China's latest five-year plan for the 'rule of law' within China, recent guidance from the State Council, and a draft Social Credit Law, which demonstrates the direction of the social credit system.

But what is exactly the Social Credit System ? If commentary in the western media is anything to go by, it is a somewhat mysterious and scary rating system. In 2018, former US Vice-President Mike Pence, sounded the alarm bells about China's social credit system, stating "China's rulers aim to implement an Orwellian system premised on controlling

virtually every facet of human life" – the so-called "social credit score." Western media outlets have spoken of the "sinister social credit system" and a system of "total control".

The term "social credit" doesn't have a precise meaning; it is an intentionally broad and vague term allowing for maximum policy flexibility. It refers to a "diverse network of initiatives aimed at enhancing the amount of 'trust' within Chinese society."

The system began with a focus on financial creditworthiness, similar to credit scores used in western countries, and moved on to include compliance and legal violations. The eventual 'end-state' of the system is a unified record for people, businesses, and the government, which can be monitored in real-time. In more recent years, policy development for the social credit system has moved beyond considerations of financial creditworthiness and compliance to encompass a broader notion of 'trust'. A common theme in the policy documents establishing the social credit system is the term '*Chengxin*', translated as 'trustworthiness', 'honesty', 'integrity', 'sincerity' or 'morality', depending on the context. More specifically, through facilitating trust, the China social credit system supports the following goals :

Firstly, it supports financial creditworthiness (zhengxin 徵信).

As in most countries, firms and individuals need a way of assessing whether others are a safe bet for lending/extending goods on credit. The social credit system aims to rectify this gap in China's financial and business ecosystem.

Secondly, the system supports judicial enforcement (gongsi gongxin 司法公信). Enforcement of judicial decisions (such as judgement debts) has proven particularly difficult in China. Part of the purpose of the social credit system is to find new enforcement mechanisms for existing laws and court decisions.

Thirdly, Commercial trustworthiness (shangwu chengxin 商务诚信) is a fundamental aspect. This means improving compliance and anti-fraud mechanisms for commercial enterprises, and those who participate in them.

Moreover, societal trustworthiness (*shehui chengxin* 社会诚信) is just as important. This covers the broader goal in the social credit system of supporting a more 'moral' society. We see this goal at work in social credit initiatives which value honesty, hard work and devotion to family.

Finally, government integrity (*zhengwu chengxin* 政务诚信) is another objective. The social credit system is 'self-reflective': bureaucrats and politicians themselves will be subject to the regime, with the goal of reducing corruption.

These ambitious goals are to be achieved via three key mechanisms. Firstly, data gathering and sharing. The fundamental building block of the social credit system is data. Through the system, data is gathered by central, regional and municipal government bodies, as well as private actors, and shared. 'Big data' algorithms are then used to process that data in a meaningful manner. Secondly, "blacklists" and "redlists" are elaborated. The data acquired is used to add individuals and corporations/businesses to lists (some publicly published, some kept more secret). Thirdly, punishments, sanctions and rewards are put in place, based partially by the presence on lists previously mentioned.

The elements of the social credit system outlined above are put into place by a variety of actors. The social credit system is, at the highest level, driven by the State Council,

currently chaired by Premier Li Keqiang. This is the most powerful administrative body within the Chinese government. It is assisted in this task by the National Development and Reform Commission (NDRC). This is a macroeconomic policy body, immediately subordinate to the State Council, and has a mixture of what would in other countries be called Treasury and Reserve/Central Bank Powers. The People's Bank of China (PBoC) also plays a prominent role at the highest policy level.

Also, dozens of central government departments and agencies have implemented elements of the social credit system, especially the blacklists and redlists. Prominent examples include the Ministry of Transport, Ministry of Culture and Tourism and the PBoC. The Supreme People's Court has also introduced an expansive blacklist of debtors under the scheme.

Regional and municipal governments play an important role too in the implementation of the system. For example, some cities decided to test the system in advance, being part of the "model cities" initiatives introduced in 2017.

Finally, several private companies have developed their own credit systems (such as Alibaba's affiliated 'Sesame Credit'). Some of these have been developed independently, while others have been developed as part of government trials. In other cases, private companies have been contracted to provide the infrastructure supporting the credit system such as Baidu's refresh of the 'Credit China' webportal, and Tencent's development support for the app.

But how does China's Social Credit System work ?

The China social credit system rates individuals based on the aggregation and analysis of data. In some trials, this has involved a single numerical score (usually between 1 and 1000), or a letter grade (usually from A-D). This information is acquired from a range of sources including individual businesses (including 'big tech') and government entities. Some of the information is isolated, and accessible only by the regional or central government authority. But in many cases, the information is shared with other regulators through a centralized database.

As the China social credit system is still in a state of evolution, it is impossible to say with certainty what exactly the negative consequences are. That said, based on those elements that are currently in place, as well as existing regional pilots, potential negative effects of a bad score once fully implemented include first of all travel bans. China's National Public Credit Information Center released a report in 2019 that said it stopped 17.5 million people from buying airplane tickets and 5.5 million from hopping on a train in 2018 because they had low "social credit" scores.

Worryingly, a low score on the SCS also impacts education for students. It may prevent some of them from attending certain universities or schools if their parents have a poor social credit rating. For example, in 2018 a student was denied entry to University due to their father's presence on a debtor blacklist. Indeed, the father failed to pay back a loan of 200,000 renminbi (around $30,000 or £23,000) after two years. He was warned by judges that punishments could be held on his children; warning that he ignored, until he and his son were surprised when they learned that the Beijing-based university which the son was applying for rejected his candidacy due to his father's low score on the SCS.

The punishment can also be extended to much further in life. Effectively, employers will be able to consult blacklists when making their employment decisions. In addition, it is possible that some positions, such as government jobs, will be restricted to individuals who meet a certain social credit rating.

Moreover, the SCS means increased scrutiny. Businesses with poor scores may be subject to more audits or government inspections.

Finally, but not less importantly, public shaming can be used. In many cases, regulators have encouraged the 'naming and shaming' of individuals presented on blacklists.

Blacklisted debtors displayed on a LED screen in Taishan city : (picture from The Conversation)

Similarly to this photo, people who do not behave like a "trustworthy citizen" may end up being displayed on public screens to be named and shamed. It is a very common practice in China to force people to be on the right track.

So far we have made several references to the 'blacklists' and 'redlists' associated with the China social credit system. China currently has a number of national and regional blacklists based on various types of violations. It is expected that over time, the system of blacklists will be fully integrated with the social credit score.

Businesses can be placed on a blacklist due to a particular violation or because of a poor social credit score. A government notice released in 2016 encourages businesses to consult the blacklist before they hire someone or assign them a contract, which goes back to what we said earlier about punishments. Companies however will not be blacklisted automatically for compliance failures. The corporate social credit system also maintains an irregularity list. This list deals with significant (but not yet 'blacklist' level), non-compliance. Presence on this list means the business is in danger of being blacklisted and should quickly take steps to improve its reputation though.

While the China Blacklisting system is still in its early stages, it is already the most prominent system of its kind worldwide. Most of the blacklisting that has occurred to date

has been as a result of violations or misbehavior of companies and the individuals working for them.

In its current iteration, the blacklisting system is highly complex. Instead of having a single blacklist used by the federal government, there are currently hundreds of blacklists being controlled by various state agencies around China. Every agency has its own jurisdiction in which it operates, giving these localized organizations the ability to blacklist individual citizens and companies that operate within their area of authority. It is important to note that being blacklisted under one agency's jurisdiction may leave the affected party subject to blacklisting from the remaining agencies across the country (the level of integration of blacklists differs across the country and between different government departments). It typically takes 2 to 5 years to be successfully removed from a blacklist, which often has a negative impact on the privileges afforded to those individuals and businesses in society. Early removal from the list is a possibility for some, depending on the severity of the offense and whether the offending party has done enough to rectify the situation in the eyes of the relevant governing body.

According to data published on the China Credit website, from June 2018 to May 2019 1.3 million firms and 2.2 million people were added to various government blacklists. During the same time 813,000 firms and 1.56 million people were removed.

In addition to being used as a metric for punishing citizens and companies for violating the country's guidelines, the social credit system is also intended to be useful in China's search for signs of potentially harmful behavior before it even occurs. "Autocratic governments would like to be able to predict the whereabouts, thoughts, and behaviors of citizens. And AI is fundamentally a technology for prediction.", said David Yang, associate professor of economics at Harvard, hostile to the Chinese system.

On the other end of the spectrum, there are positives of the social credit system for people and corporations who are determined to be outstanding members of Chinese society. In this context, the opposite of being blacklisted is to be "redlisted". Redlisting allows citizens and companies to access certain privileges that will impact their day-to-day lives. "Redlisted" individuals may receive benefits like parking and public transit discounts or discounts on tourist site tickets for example. "Redlisted" companies can also have multiple benefits as a reward of their good compliance with rules. First, companies that are classified as an 'Advanced Certificate Enterprise' may receive faster customs clearance. 'A-rated' tax-payers may have their tax returns processed more quickly. They may also have fewer inspections and audits by the authorities.

As we are constantly developing more and more elaborate technologies, they are poised to play a large role in the country's social credit system. Artificial Intelligence (AI) facial recognition software is said to be utilized in tandem with over 200 million surveillance cameras in China in 2018. According to the Wall Street Journal, this number was supposed to reach 560 million by 2021. Today, as of 2023, there are 700 million, which means there is roughly one CCTV camera for two Chinese citizens. China is the country where there are the most cameras in the world. As soon as a person gets out on the street, they will inevitably be filmed/caught on camera. They are omnipresent.

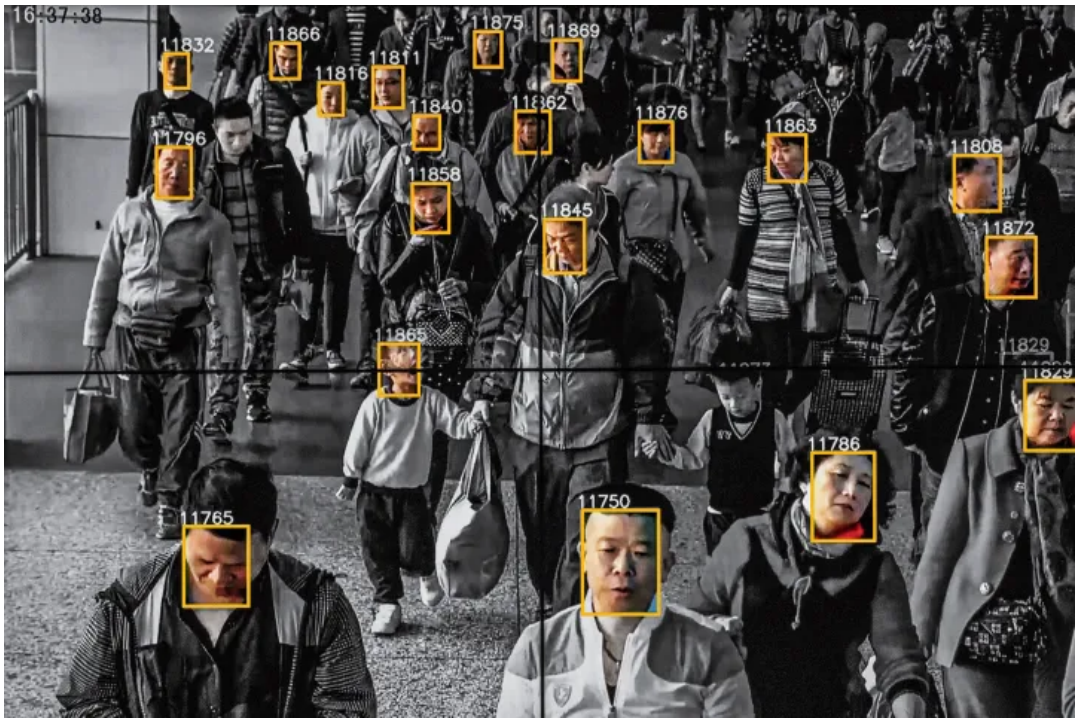
Security cameras looking over Tiananmen Square, Beijing. : Ed Jones/AFP/Getty Images

In order to avoid these cameras, many experiments were made by a number of citizens. Namely, one was made in October 2020 by a man called Deng in Beijing. He recruited a handful of participants, whose mission was to walk Happiness Avenue by dodging any CCTV. The result was staggering : it took them more than two hours to walk 1.1 km (0.7 mile), the length of the avenue, without their face being caught on camera.

Deng and several participants crouch to avoid being caught by a surveillance camera. : Photo taken from BBC article.

"It was harder than I had expected," told volunteer Joyce Ge, 19, to BBC News. She added : "I thought there were just a few cameras and I could easily duck and cover. But it turned out not to be the case at all. The cameras were really all over the place, and it was impossible to evade them."

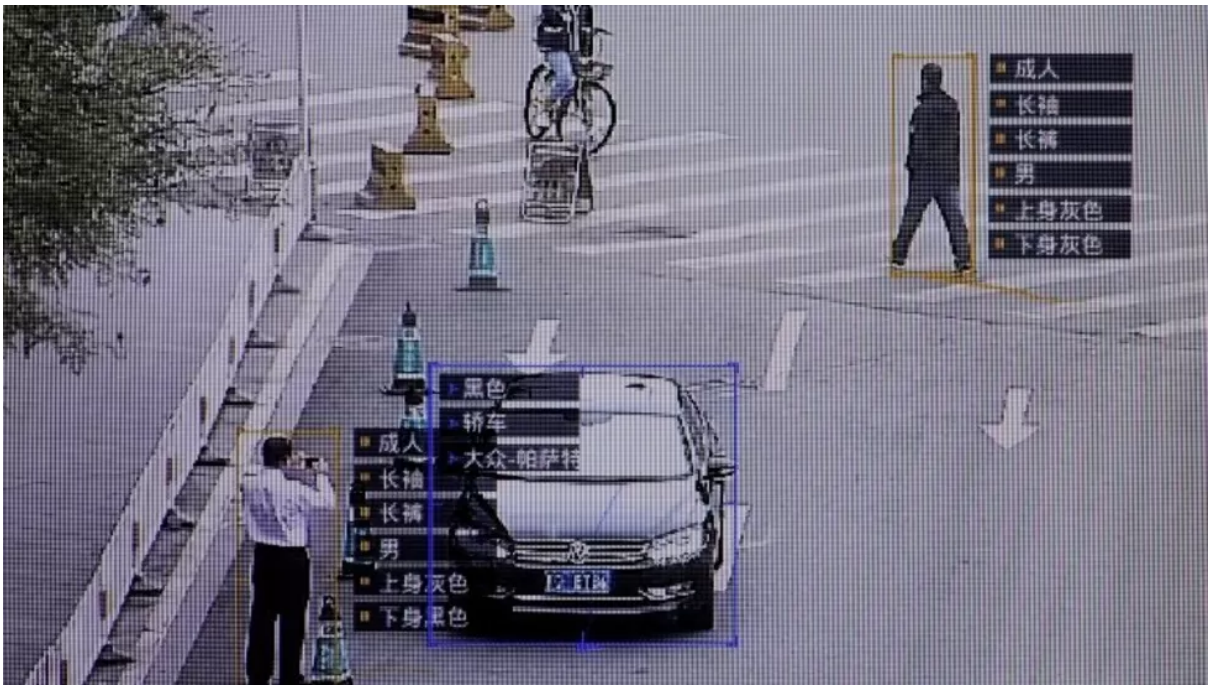
Moreover, AI is used through the CCTV cameras for facial recognition, to recognise in real time the people that are being filmed :



Facial recognition is one element of China's expanding tracking efforts : Photo-Illustration by TIME: Source Photo: Gilles Sabrié—The New York Times/Redux

From that facial recognition, the authorities have direct access to the person's essential information :

Critics say China's surveillance cameras are being used to identify personal information : Reuters (extracted from a BBC article)

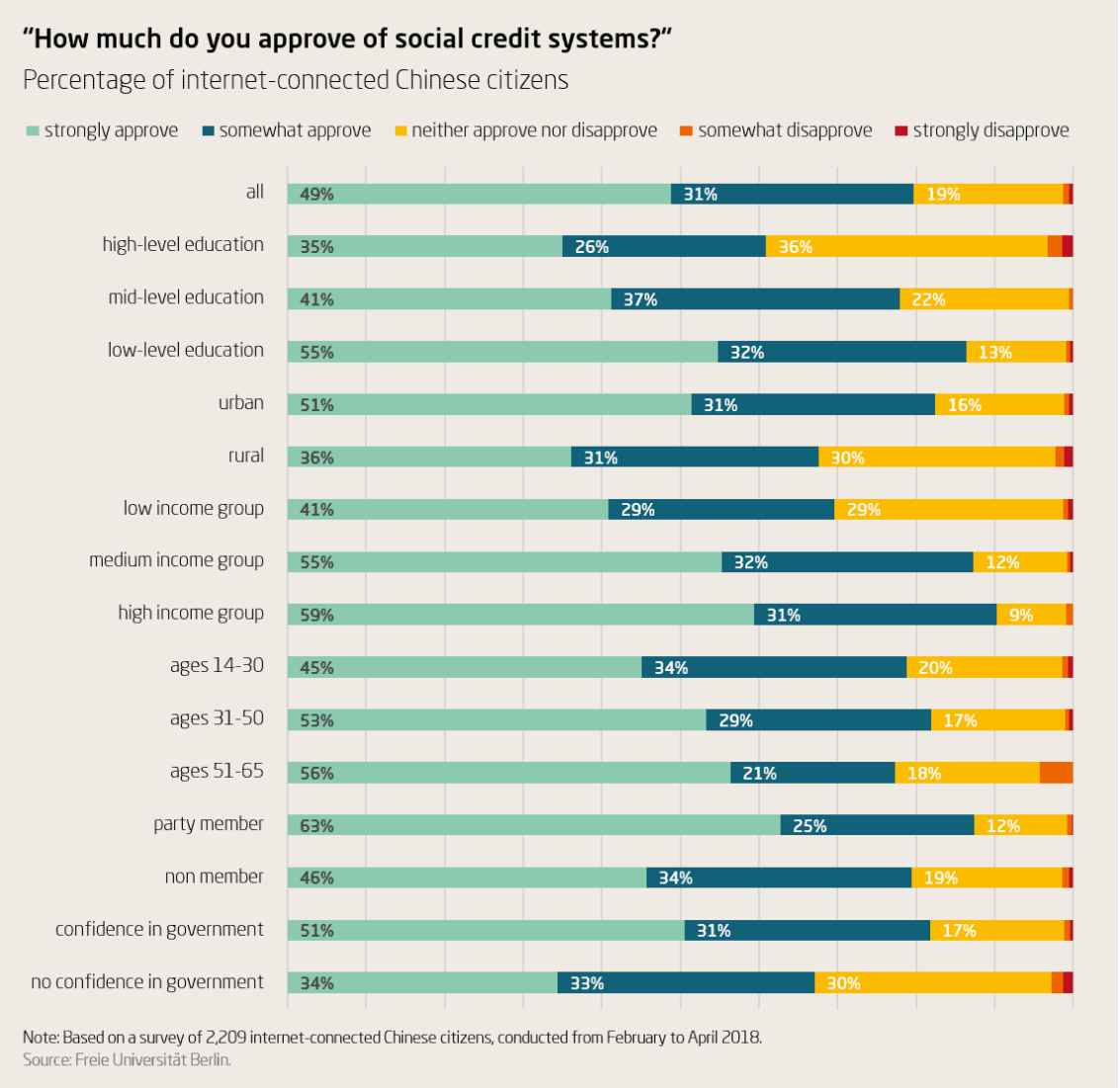


Some argue that the purpose of large-scale surveillance measures is to give Chinese officials the ability to track their citizens in every facet of everyday life, collecting masses of data to determine whether an act worthy of being blacklisted has occurred.

Along with these physical surveillance measures, the Chinese government continues to track the online behaviors of its citizens. There are a plethora of violations Chinese officials may be looking for, including evidence of writing and sharing anti-government ideologies. The AI software is able to do the majority of this work on behalf of the government and alert officials when a violation has occurred. The technology has advanced to a place where the AI can identify videos of anti-government protests and block users from viewing them.

What is the public perception of the Social Credit System ?

Although there has been substantial resistance to the social credit system from a global perspective, it appears that most Chinese citizens approve of the system. Those most familiar with the social credit system, citizens and businesses in China, are widely supportive of the system.



This study conducted by the Freie Universität in Berlin shows how strong support the SCS benefits from. Effectively, 80% of respondents either somewhat approved or strongly approved of social credit scores. Just 1% of participants reported either strong or some degree of disapproval in the system. And whatever the age, level of education, the area they live in (etc.), people overwhelmingly approve of the system. However it is important to note that this survey only represents Chinese internet users that participated in the survey and is not necessarily a representation of how the country feels as a whole; although it does give a good idea.

This could be explained by the fact that many people see in the social credit a way to climb the social ladder, to rise through the hierarchy; because if they behave well according to the standards of the government, they will have access to new privileges and luxuries.

In hindsight, the Chinese social credit system aims to be an all-encompassing system for assessing the trustworthiness of individuals, corporations and government actors within China. To date, there is no unified, 'social credit score' held on each individual assessing their trustworthiness. Rather, there are a range of different ratings held by government departments, and individual municipal and provincial governments. However, there is an increasing level of cohesion across China with social credit ratings due to centralized information platforms. This is especially the case for corporate social credit ratings and the blacklists that relate to those ratings.

The program's slogan "once you lose trust, you will face restrictions everywhere" seems perfectly accurate, because from the moment an individual commits a breach, his social score will diminish, which restricts the ability to do certain activities or access to certain things. Therefore some serious human rights problems are created.

While the Chinese system is the most developed at the moment, such systems could see the light of day in other parts of the world as AI is developing at an extremely rapid rate; it will be a determining factor to define a country's power.

However, it is unlikely that any social credit system like China's will exist in Europe, specifically in the European Union (EU), despite its plan to develop AI. While the EU is supportive of AI, it is also the first organization in the world to regulate it. The goal is to make "safe and transparent" AI, therefore being in opposition to China's model. Earlier this year, in June 2023, Members of European Parliament (MEPs) voted in favor of different rules in response to the AI Act proposed by the European Commission in 2021.

The new rules establish obligations for providers and users depending on the level of risk from artificial intelligence. While many AI systems pose minimal risk, they need to be assessed. Several categories have been created :

First of all, there are systems that could pose an "unacceptable risk". "Unacceptable risk" AI systems are systems considered to be a threat to people and will be banned. They include "cognitive behavioral manipulation of people or specific vulnerable groups", for example voice-activated toys that could encourage dangerous behavior in children. Social scoring is also considered as an "unacceptable risk", classifying people based on behavior, socio-economic status or personal characteristics. Thirdly, real-time and remote biometric identification systems, such as facial recognition are to be prohibited within the Union. This goes to confirm the fact that no such systems as China will emerge in Europe. Some

exceptions may be allowed: for instance, “post” remote biometric identification systems where identification occurs after a significant delay will be allowed to prosecute serious crimes but only after court approval.

The slightly less dangerous category is the “high risk”, which are AI systems that negatively affect safety or fundamental rights. They will be divided into two categories. The first one is AI systems that are used in products falling under the EU’s product safety legislation. This includes toys, aviation, cars, medical devices and lifts namely. The second category groups many subcategories :

- “Biometric identification and categorisation of natural persons”
- “Management and operation of critical infrastructure”
- “Education and vocational training”
- “Employment, worker management and access to self-employment”
- “Access to and enjoyment of essential private services and public services and benefits”
- “Law enforcement”
- “Migration, asylum and border control management”
- “Assistance in legal interpretation and application of the law”

All high-risk AI systems will be assessed before being put on the market and also throughout their lifecycle.

Next comes the “generative AI” category. Generative AI, like ChatGPT, would have to comply with transparency requirements:

- Disclosing that the content was generated by AI
- Designing the model to prevent it from generating illegal content
- Publishing summaries of copyrighted data used for training the system

Finally, there are “limited risk” AI systems that should comply with minimal transparency requirements that would still allow users to make informed decisions. After interacting with the applications, the user can then decide whether they want to continue using it. This includes AI systems that generate or manipulate image, audio or video content, for example deepfakes.

This series of measures which is to put in practice over the next few years comes follows on from existing measures and plans in the EU to protect the user’s privacy, the most important one being the General Data Protection Regulation (GDPR) which aims to protect user’s personal data and make sure that private businesses process in a secure and ethical manner.

GDPR replaces the EU Data Protection Directive of 1995. The new directive focuses on keeping businesses more transparent and expanding the privacy rights of data subjects.

GDPR governs the way in which we can use, process, and store personal data (information about an identifiable, living person). It applies to all organizations within the EU, as well as those supplying goods or services to the EU or monitoring EU citizens. Therefore it is essential for businesses and organizations to understand explicitly what GDPR means. It is the legislative force established to protect the fundamental rights of data subjects whose personal information and sensitive data is stored in organizations. Data subjects will now have the right to demand subject access to their personal information, and the right to demand that an organization destroys their personal information. These regulations will affect most sectors within business, from marketing to health services. Therefore, to avoid the crippling fines administered by the Information Commissioner's Office (ICO) it is essential to become GDPR compliant.

Although it does replace the previous directive from 1995, it is largely based on it; still bringing important changes nonetheless.

Firstly, its territorial scope is increased. The GDPR applies to all companies processing the personal data of data subjects residing in the EU/EEA, regardless of the company's location. To elaborate, the GDPR applies to the processing of personal data by controllers (companies) and processors (entities that process the data for the companies) in the EU/EEA, whether or not the processing itself takes place in the EU/EEA. The GDPR will also apply to the processing of personal data of data subjects in the EU/EEA by a controller or processor not established in the EU/EEA. In essence, all companies and organizations all over the world are affected as long as they process personal data of EU citizens.

Secondly, organizations and companies found to be in breach of GDPR will be fined according to the scope and type of their infringement. A supervisory authority will assess the violation (e.g., shortcoming, data breach) in order to determine what type of penalty will be imposed. It follows a tiered approach to fines. The first penalty tier is set at up to 10 million euros, or in the case of an undertaking, up to 2 percent of the company's global annual turnover of the preceding financial year, whichever amount is higher. The second tier is set at up to 20 million euros, or in the case of an undertaking, up to 4 percent of the company's global annual turnover of the preceding financial year, whichever is the higher amount. This is the maximum fine that can be imposed, as outlined in Article 83 of the GDPR, on companies found and proven to have violated specific GDPR provisions by appointed supervisory authorities of the GDPR.

Thirdly, the directive imposes clearer and concise consent. Organizations and companies will no longer be allowed to use long and illegible terms and conditions and complex forms to request consent from customers. Such forms must be given in an intelligible and easily accessible format, using clear and plain language. Consent must be explicitly given and customers must also be able to easily withdraw that consent.

Moreover, organizations and companies must notify supervisory authorities and their customers in the event of a data breach that is likely to place at risk the rights and freedoms of individuals. This notification, which needs to happen within 72 hours after the discovery of a breach, will be mandatory. This also applies to data processors that need to notify their customers.

Also, data subjects will be able to obtain confirmation from companies as to whether or not their personal data is being processed, where, and for what purpose. The company must also provide a copy of the customer's personal data at their request, free of charge.

Furthermore, the 'right to be forgotten' allows the data subject to have the company erase his or her personal data. This right to data erasure is not absolute and can be claimed under certain conditions: withdrawal of consent; the data is no longer relevant to the original purposes of processing. This right is subject to public interest or national security concerns

Additionally, privacy by design and by default becomes mandatory. It means that each new service or business process that makes use of personal data must take the protection of such data into consideration. Privacy by default simply means that the strictest privacy settings automatically apply once a customer acquires a new product or service. This means no manual change to the privacy settings should be required on the part of the user to select the strictest setting. The GDPR is making privacy by design a major provision and, as a consequence, the inclusion of data protection as a key design element becomes an integral objective of any system design, at the very onset.

Finally, in organizations and businesses, the position of "Data Protection Officer" (DPO) has to be created. In addition to supporting an organization's compliance with the GDPR, the DPO will have the essential role of acting as an intermediary between the organization and supervisory authorities, data subjects, etc. Not every organization/company will need a DPO; there are certain criteria that determine whether a DPO is required or not.

In a nutshell, an important consequence of these regulations, apart from making companies and organizations enforce stronger data protection and overall security posture, is also the streamlining of efforts across different industries and sectors all over the world.

WHAT SHOULD RESOLUTIONS BE ABOUT?

In order to know the stance of the represented country regarding the debated issue, it is important to first assess its current situation.

- What is the current regime of your country? (Democracy, dictatorship, authoritarian regime, hybrid regime, monarchy…)
- What is this regime's consideration of Human Rights? (The Human Rights Index - 'HRI' - is a good indicator of this question)
- What is your country's level of income/development? (MIC, LIC, HIC/High, medium, low)
- How well is your country integrated into cyberspace? How important is your country's Internet penetration?
- Is it in the current regime's interest to extend or reduce the digital privacy of its citizens?

- Has the country started its digitalization? If so, how far gone is it?

After having assessed the economic, social and political situation of the country, it is now possible to study the debated issue in itself in depth.

- Considering the type of regime ruling your country and its interests, what is your country's stance about the access to the Internet being considered as a fundamental right?
- Would the country benefit from a severe regulation of the major companies or private actors operating in the Internet and cybertechnologies sector?
- Is the country ready, capable and willing to enforce a strong legislation regarding the digital privacy of its citizens?
- How does the country already ensure its citizens digital privacy while fighting criminal behaviors in cyberspace? What are the country's future plans in that regard?
- Is the country opposed to regulation in cyberspace as a limit to their digital sovereignty or is the country willing to develop a global functional governance of the cyberspace ensuring the digital privacy of the citizens of the United Nations?

BLOC POSITIONS

Afghanistan:

GDP: $14.79 bn (2021)

HDI: 0.478

HRI : 0.04

Percentage of the population using the Internet: 18.4% (2020)

In 2014, Afghanistan launched its first cybersecurity policy: the National Cybersecurity Strategy of Afghanistan (NCSA). It reckoned adapting to the challenges brought by new technologies, and aimed to develop a safe, secure and resilient cyberspace for the government and the citizens. Its missions were to to protect and assure data, information and IT infrastructure security in Afghanistan's cyberspace, enhance capacities to prevent and response to cyber threats, protect the children and youth of Afghanistan in cyberspace, mitigate the risk of vulnerability, damage from cyber threats and incidents through a variety of standardized institutional structures, policies, procedures, people, technologies and administrative processes. Despite such efforts, the country remains at an all time low regarding cybersecurity, and since the return of the Talibans to power in 2021, the country lost 37 places in the rankings of cybersecurity, dropping in free fall from 108th to 145th.

China:

GDP: $17.73 trillion (2021)

HDI: 0.768

HRI : 0.17 (2022)

Percentage of the population using the Internet: 76.4% (2023

In China, data protection is covered by the Personal Information Protection Law (PIPL) which shares many similarities with Europe's GDPR. Both GDPR and PIPL cover data privacy in a very wide sense, including 'extraterritorial' applications, where citizens' data is recorded or processed outside the borders of the EU or China. Both laws use the concept of consent as a primary legal justification for the use of individual data. In common with GDPR, PIPL requires that companies must limit personal information gathering to the minimum amount required by the data's purpose. In the case of individuals, both GDPR and PIPL allow people to access data held on them, withdraw consent for companies to hold or use their data, or ask for it to be corrected or deleted. Both laws require companies to take measures to protect any personal data they hold, and as part of this to employ a Data Protection Officer above certain levels of data processing or in circumstances that cover most businesses. As with the GDPR, this may require a Data Processing Agreement be in place between a company that controls the data and any third party that processes it. Aside from any criminal charges or other legal remedies, both GDPR and PIPL allow non-compliant companies to be given large fines for breaches of the law. However, there are also key differences. The authority for GDPR in each member state is held by an independent regulator. In contrast, the PIPL is overseen by a state-backed regulator, the Cyberspace Administration of China (CAC). In addition, PIPL does not restrict the Chinese state's ability to access and use citizens' personal data. GDPR does influence how national governments handle data, which might be covered by several legal bases in the GDPR including via the legal basis of legitimate interests, which does not exist in the PIPL. Finally, the GDPR has its roots in the rights of individuals to own and control their personal data, and is not aligned with the political aims of EU member states or the EU as a bloc. PIPL, however, aligns with and reinforces the political and national security aims of the Chinese state.

Democratic Republic of Congo:

GDP: $55.35 bn (2021)

HDI: 0.571

HRI : 0.27 (2022)

Percentage of the population using the Internet: 22.9% (2023)

In November 2019, the Congolese government passed the 'Law on the Protection of Personal Data', which aims at lessening accidents caused by the violation of private information stocked on the Internet. The 'Law' is very similar to the EU's General Data Protection Regulation (GDPR), mainly because it states that a Commission will soon be implemented through the legislation to guarantee the protection of data. However, the issue is that this Commission still has not been established. Moreover, in mid-2023, a new prohibition has been enacted, on using personal data to harm and threaten people's reputation, yet no sanction for it has been clearly mentioned.

Ghana:

GDP: $77.59 bn (2021)

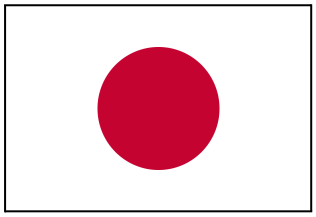
HDI: 0.63

HRI : 0.89

Percentage of the population using the Internet: 53% (2022)

Recognizing the importance of safeguarding data subject rights, data controller responsibilities, and regulatory efficiency in the realm of technology, Ghana acknowledges the necessity for a robust legal framework to protect data subject privacy while enabling technology implementation by data controllers. Ghana's digital landscape has experienced impressive advancements in recent years, revolutionizing various aspects of the nation. The integration of digital technologies and platforms in Ghana has not only streamlined business operations but has also exerted a profound influence on the logistics sector. A key catalyst for this transformation stems from the widespread usage of mobile phones, internet connectivity, and digital payment systems across the nation.Ensuring the security of your systems and proactively addressing data privacy concerns on an enterprise scale can indeed incur substantial costs. However, the potential repercussions of a data breach are so substantial that it becomes imperative to make well-considered investments.

Japan:



GDP: $4.941 trillion (2021)

HDI: 0.925

HRI : 0.93

Percentage of the population using the Internet: 94% (2022)

In Japan, The Act on the Protection of Personal Information Act No. 57 of 2003 (“APPI”) is the primary legislation that applies to the collection and processing of personal data. This law went through substantial revision both in 2017 and 2022. Japan’s APPI is a federal personal information protection law to regulate the handling of personal information by individuals and organizations, including government agencies, businesses, and nonprofits. The Act is overseen by the Personal Information Protection Commission (PPC), an independent administrative body founded in 2005, after the APPI had been in effect for two years. The APPI requires organizations that want to collect personal information to obtain consent from individuals prior to collecting, using, or sharing it, but only in some cases, like if the information is sensitive or is to be transferred to a third party or outside of Japan. More in line with laws in the US, in many cases the APPI does not require consent for collection or use for personal information that is not sensitive or meets other criteria.

Kazakhstan:

GDP: $197.1 bn (2021)

HDI: 0.811

HRI : 0.52

Percentage of the population using the Internet: 85.9% (2022)

Data protection has been a significant area of interest for the Government of the Republic of Kazakhstan ('the Government'). At present, the Law of the Republic of Kazakhstan of 21 May 2013 No. 94-V on Personal Data and its Protection ('the Personal Data Law') provides general regulations on the collection and processing of personal data and notably includes broad requirements for data localization. In addition, the Laws on Amendments to the Personal Data Law were introduced in January and December 2021, July, November, and December 2022, significantly extending data protection obligations for organizations. Those amendments introduce, among other things, further requirements for personal data collection and processing, and obligations for data operators (similar to data processors). Those amendments further establish the competency of the personal data protection authority including its powers and role.

Mali:

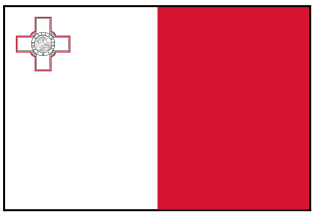
GDP: $19.14 bn (2021)

HDI: 0.428

HRI : 0.74 (2022)

Percentage of the population using the Internet: 34.5% (2023)

Mali makes it a point of honor to preserve the safety of personal data storage, as it created in 2016 the Autorité de Protection des Données à caractère Personnel (APDP) as a condition to the Data Protection Act that passed the same year, ensuring Malians have the right to privacy and to fundamental rights regarding the protection of their data. This law is reviewed every March 21st of each year, making it always up to date with the latest challenges brought by the ever growing development of technology. Thanks to this law, Malians, among other things, have the right to access their data, refuse their use for prospection by various companies and agents and correct or even delete some information.



Malta:

GDP: $20.311 bn

HDI: 0.918

HRI : 0.9 (2022)

Percentage of the population using the Internet: 87% (2021)

Malta is one of the most advanced countries in the European Union (EU) in the digital domain. The country has, effectively, successfully started its digitalization and aims to have a leadership in the cybernetic domain at the scale of the EU. The Internet penetration of the

country is very strong, and as a developed, democratic country Malta's internet is free of political control or regulation, and easy to access for its citizens. The country is one of the most advanced/on-edge countries of the EU regarding the access to Internet, with maltese Members of the European Parliament (MEP) advocating for its recognition as a human right (MEP Josianne Cutajar: "It's high-time for internet access to be recognised as a fundamental right"). As a member of the EU, Malta follows and supports the General Data Protection Regulation (GDPR), ensuring a strong and unquestionable digital privacy for its citizens from private (and most public) actors, enforced by the support of the European Union Agency for Cybersecurity (ENISA).

Mexico:

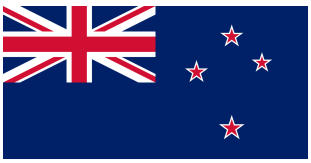
GDP: $1.811 trillion

HDI: 0.758

HRI : 0.68 (2022)

Percentage of the population using the Internet: 78% (2023)

The Federal Law on the Protection of Personal Data held by Private Parties (Ley Federal de Protección de Datos Personales en Posesión de los Particulares) ("the Law") entered into force on July 6, 2010. Subsequently, the Executive Branch has also issued many regulations for other matters referred to herein as "Mexican Privacy Laws". Mexican Privacy Laws apply to all personal data processing under any of the following circumstances: processing carried out by a data controller established in Mexican territory; processing carried out by a data processor, regardless of its location, if the processing is performed on behalf of a data controller established in Mexico; processing by or on behalf of a data controller not located in Mexico, where Mexican legislation is applicable pursuant to the execution of an agreement or Mexico's adherence to an international convention; or Processing carried out within Mexican territory, on behalf of a data controller not established in Mexican territory, unless such processing is only for transit purposes. The Law only applies to private individuals or legal entities that process personal data, and not to the government, credit reporting companies governed by the Law Regulating Credit Reporting Companies or persons carrying out the collection and storage of personal data exclusively for personal use where it is not disclosed for commercial use. Furthermore, Mexican Privacy Law also does not generally apply to business-to-business data.



New Zealand:

GDP: $249.9 bn (2021)

HDI: 0.937

HRI : 0.96 (2022)

Percentage of the population using the Internet: 94% (2023)

The Privacy Act 2020 (Act) governs how agencies collect, use, disclose, store, retain and give access to personal information in New Zealand. It contains 13 Information Privacy Principles (IPP) that govern the use of personal information in New Zealand. The Act gives the Privacy Commissioner the power to issue codes of practice that modify the operation of

the Act in relation to specific industries, agencies, activities or types of personal information? But also gives him guidelines on protecting online privacy. Moreover, as mentioned in the IPP 9, personal information may not be kept indefinitely. Agencies are therefore required not to retain personal information for longer than is necessary for the purposes for which it may lawfully be used.

Other than compliance with the Act, no additional legislation deals with the collection of location and traffic data by public electronic communications services providers and use of cookies.

Notably, New Zealand was the first APAC (Asia Pacific region) jurisdiction to be recognised as providing an adequate level of personal data protection by the European Commission.

North Korea:

GDP: $17.365 M

HDI: 0.733 (2008)

HRI : 0.02

Percentage of the population using the Internet: nearly 0%

North Korea is probably the most isolationist country in the world, which of course reduces the use of the internet to almost 0%, since its main use is to link people - and data - all throughout the globe. North Korean institutions are made durable in their particularity of not requiring access to the internet. Most North Koreans only know about the internet in theory, but do not quite understand how it works or even is. This service is exclusively reserved for a few lucky thousands inhabitants, but even their access to it is limited and strictly regulated.

Russia:

GDP: $2.24 trillion

HDI: 0.822

HRI : 0.31 (2022)

Percentage of the population using the Internet: 89% (2022)

Fundamental provisions of data protection law in Russia can be found in the Russian Constitution, international treaties and specific laws. Russia is a member of the Strasbourg Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention) (ratified by Russia in 2006) and the Russian Constitution establishes the right to privacy of each individual (articles. 23 and 24). Most rules are found in specific legislation, particularly the Data Protection Act No. 152 FZ dated 27 July 2006 (DPA) and various regulatory acts adopted to implement the DPA as well as other laws, including the Information, Information Technologies and Information Protection Act No. 149 FZ dated 27 July 2006 establishing basic rules as to the information in general and its protection. In addition, the Russian Labour Code contains provisions on the protection of employees' personal data (Part XIV). Other laws may also contain data protection provisions which

implement the provisions of DPA in relation to specific areas of state services or industries. On 22 July 2014 notable amendments to the DPA were adopted and came into force on 1 September 2015. The amendments require all personal data operators to store and process any personal data of Russian individuals within databases located in Russia (subject to few exceptions). The penalty for violation of this requirement is ultimately the blocking of websites involving unlawful handling of Russian personal data. However, Russian law does not specifically regulate online privacy. The definition of personal data under the DPA is rather broad.

Sudan:

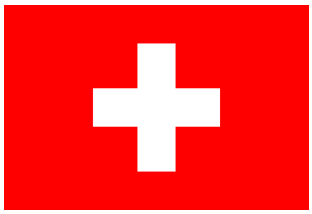
GDP: $51.66 bn (2023)

HDI: 0.508

HRI : 0.31 (2022)

Percentage of the population using the Internet: 30.9% (2022)

The Republic of Sudan doesn't have a publicly published strategy on cybersecurity. The Sudan Computer Emergency Response Team (Sudan CERT) is the first responder to information security incidents. It is also responsible for raising security awareness for companies, institutions and all national facilities and to protect them against cyberattacks. Also, it acts as an advisory body to citizens and companies in information security before and after cyber-attacks, as well as traces the criminals of cyberattacks and hand them over for trial under existing laws. One year after having put in place a cybercrime legislation (through the Computer Crime Act of 2007), Sudan established its first Attorney General for Cyber Crimes (2008). The new Combating Cybercrime Act contains partial implementations of substantive law provisions, addressing illegal access, data interference and illegal interception. There is limited information available on the new Law. The new act introduces criminal penalties for the spread of fake news online. Despite efforts, the country remains much fragile in front of the challenges brought by cyberspace: its national cybersecurity index was the 127th worldwide in 2023 and it is stagnant. The country is governed by a Transitional Military Council and also has to deal with internal struggles for power. Hence, Sudan's legislation regarding cybersecurity remains very weak and unadapted.



Switzerland:

GDP: $807.71 bn (2023)

HDI: 0.962

HRI : 0.96 (2022)

Percentage of the population using the Internet: 98% (2022)

In Switzerland, the processing of personal data in the context of online services is subject to the general rules under the New Federal Act on Data Protection (FADP). This act strengthens the rights of consumers regarding their data and aligns Swiss data protection law with the EU GDPR (European General Data Protection Regulation). More precisely, the FADP sets more stringent obligations on non-Swiss companies doing business in

Switzerland. In addition, certain aspects of online privacy are covered by other regulations, such as the use of cookies which is subject to the Swiss Telecommunications Act (TCA).

Under the TCA, the use of cookies is considered to be processing of data on external equipment, suh as on another person's computer. Such processing is only permitted if users are informed about the processing and its purpose as well as about the means to refuse the processing, such as configuring their web browser to reject cookies.

Syria:

GDP: $11.16 bn (2020)

HDI: 0.577

HRI : 0.09 (2022)

Percentage of the population using the Internet: 49.2% (2022)

If Syria often makes the news with its ongoing civil war, many areas are untouched by hostilities, and daily life continues. As in any country, the internet plays a part in keeping the economy going. People still need to send and receive emails, communicate through social media, and check online news headlines. Syria is a patchwork of religions, and religious adherents can easily be incited to violence and revenge by a missing word in a social media post. So, the government is nervous about the Web's potential to create offense or organize a protest. However, social media is allowed.

Many of the attacks on dissenters and journalists in the country are committed by the Turkish authorities that control the north of the country or the Suni rebels who dominate rural areas.There is a lack of cybersecurity awareness in Syria, which is surprising, given that the country is in a state of conflict. The lack of interest by Syria's government in promoting a cybersecurity policy to businesses and public sector agencies probably lies with the nature of those who oppose the government with the most vigor – they are fundamentalists who condemn the use of technology.

VPNs are legal in Syria, as are encrypted chat apps, such as Signal, Telegram, and WhatsApp. In October 2018, the Syrian Telecommunications and Post Regulatory Authority (SY-TPRA) revealed that it was considering a ban on VoIP services. This was mainly because the free international voice and video call these services offered undermined the state-owned telecoms provider, Syrian Telecom. However, that ban was never implemented.

Like many countries in the world, Syria has legislation against cybercrime. The central plank of anti-cyber terrorism legislation is the Cybercrime Law 17/2012, updated in 2018. This law established the responsibility for monitoring cybercrimes in Syria and assigned it to the National Agency for Network Services (NANS). This responsibility is implemented by CERT Syria, which is the national Computer Emergency Response Team.

Türkiye:

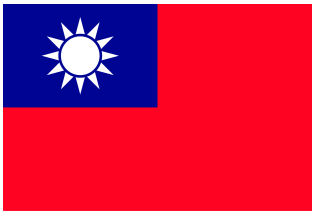
GDP: $1.154 trillion (2023)

HDI: 0.838

HRI : 0.33

Percentage of the population using the Internet: 81% (2021)

In Türkiye, the legislation enforcing and protecting digital privacy is moderate. There is no legislation in Türkiye that specifically regulates privacy in respect of cookies and location data. However, Law No. 5651 on Regulating Broadcasting in the Internet and Fighting against Crimes Committed through Internet Broadcasting enables Internet users to initiate prosecution in case of infringements of their personal rights. Further, various amendments were made to Law No. 5651 on July 31, 2020. One of these amendments was adding the term *"social network provider"* and the obligations of the social network providers have been regulated within this scope. The government also intervenes a lot in cyberspace, censoring or removing content from websites opposed to Mr. Erdogan, the President. Following the 2016 coup attempt in Türkiye, the Executive Branch adopted twenty decrees without parliamentary approval or oversight. The decrees resulted in permanent legislative and structural changes and mass dismissal of public servants, falling short of EU human rights standards. One decree grants many unspecified institutions unfettered access to communications data without a court order. The surveillance decree was designed to be used against coup plotters and so-called "terrorist organizations." Such unfettered power violates the rule of law and the Principle of Legality, necessity and proportionality under international human rights law. The decree also compels companies to comply with the Information and Communication Technologies Authority (BTK) requests. In conclusion, paranoia pushes the Turkish government to reduce its citizens' digital privacy if it means to stabilize and enforce their rule.



Chinese Taipei (Taiwan):

GDP: $790.7 bn (2023)

HDI: 0.926

HRI : 0.93 (2022)

Percentage of the population using the Internet: 90.7% (2023)

In order to protect Taiwan's population's personal data, Taiwan's government has implemented a Personal Data Protection Act (PDPA). Indeed, the National Development Council (NDC) is the authority currently in charge of interpreting the act. The PDPA was first introduced in Taiwan in 1995 and was significantly amended and renamed in 2010, finally becoming effective in 2012. As the first article mentions: "The Personal Data Protection Act [...] is enacted to regulate the collection, processing and use of personal data so as to prevent harm to personality rights, and to facilitate the proper use of personal data." The framework of the PDPA is similar to that of the privacy legislation of the EU because a key source of reference for the 2010 amendment adopted by the EU in 1995. In order to perform the relevant tasks, the NDC established a Personal Data Protection Office in July 2018. It has an important mission: obtain the "adequacy decision" from the EU authority concerning the General Data Protection Regulation (GDPR). The negotiation started in spring 2018.

Furthermore, the Constitutional Court of the Country confirmed that the right to privacy is one of the basic human rights and it is effectively protected by the constitution. The Civil Code offers general protection as well on the right to privacy, enabling individuals to bring civil liability claims for infringement of privacy.

United Kingdom:

GDP: $3.07 trillion (2022)

HDI: 0.929

HRI : 0.89 (2022)

Percentage of the population using the Internet: 93% (2023)

Following the UK's exit from the European Union, the UK Government has transposed the General Data Protection Regulation (GDPR) into UK national law (thereby creating the "UK GDPR"). In so doing, the UK has made a number of technical changes to the GDPR in order to account for its status as a national law of the United Kingdom. The Data Protection Act 2018 (DPA) remains in place as a national data protection law, and supplements the UK GDPR. It deals with matters that were previously permitted derogations and exemptions from the EU GDPR (for example, substantial public interest bases for the processing of special category data, and context-specific exemptions from parts of the GDPR such as data subject rights). Just like the EU GDPR, the UK GDPR has extra-territorial effect. As a result, an organization that is not established within the United Kingdom will be subject to the UK GDPR if it processes personal data of data subjects who are in the United Kingdom.

Yemen:

GDP: $21.61 bn (2018)

HDI: 0.455

HRI : 0.18 (2022)

Percentage of the population using the Internet: 26.7% (2022)

Under Ali Abdullah Saleh's rule, practices of repression were committed using the 1990 Press and Publications Law and the Penal Code, which restricted free speech on multiple levels under the pretext of protecting national security, religion, foreign relations, etc. Despite the low level of internet activity compared to other countries, cases of website blocking were documented and several individuals complained about surveillance of their phone calls and hacking of their email and Facebook accounts. While there were no documented cases of digital surveillance in Yemen, some cyber activists have expressed concern that if it is not already the case, surveillance technology will soon be used by the authorities, particularly the national security agency, to spy on digital communication.

While broadcast media remain the most popular method to reach the public, the internet has taken a modest share because it grants users the ability to publish, share and consume content much more easily than other forms of media. Internet usage has increased steadily since it was first introduced in 1996 by the Ministry of Telecommunication's Public Telecommunications Corporation (PTC) and Teleyemen, which was formed in 1990 as a joint company owned by PTC and the United Kingdom's Cable and Wireless plc. Today, those two companies monopolize the internet service provider (ISP) business as no private companies are allowed to operate. This has created an environment that lacks accountability and transparency and in which not many choices are provided to the public.

BIBLIOGRAPHY

1. HUMAN RIGHTS COUNCIL
2. Membership of the Human Rights Council for the 17th cycle (1 January - 31 December 2023) by regional groups | OHCHR
3. What is Data Protection and Privacy?
4. What is Artificial Intelligence (AI) ? | IBM
5. data breach
6. Social Credit System - Wikipedia
7. the Hukou system
8. China's Algorithms of Repression: Reverse Engineering a Xinjiang Police Mass Surveillance App | HRW
9. I researched Uighur society in China for 8 years and watched how technology opened new opportunities – then became a trap
10. Opinion: How to counter China's scary use of AI tech
11. judgment debt | Wex | US Law | LII / Legal Information Institute
12. China Banned 23 Million People From Traveling Last Year for Poor 'Social Credit' Scores
13. China bars millions from travel for 'social credit' offenses | AP News
14. George Soros at Davos: 5 Takeaways from His Big Speech | Fortune
15. A Chinese university suspended a student's enrolment because of his dad's bad social credit score
16. China's Social Credit System puts its people under pressure to be model citizens
17. Big Brother is watching you: How China ranks its citizens - Focus
18. The complicated truth about China's social credit system | WIRED UK
19. China's CCTV surveillance network took just 7 minutes to capture BBC reporter | TechCrunch
20. How to 'disappear' on Happiness Avenue in Beijing - BBC News
21. Big Brother is watching: China has one surveillance camera for every 2 citizens!
22. How China Is Using Big Data to Create a Social Credit Score | Time.com
23. I researched Uighur society in China for 8 years and watched how technology opened new opportunities – then became a trap
24. China: Freedom on the Net 2021 Country Report
25. The great firewall of China: Xi Jinping's internet shutdown
26. the EU's product safety legislation
27. AI rules: what the European Parliament wants | News
28. 52018DC0237 - EN - EUR-Lex
29. Europe moves ahead on AI regulation, challenging tech giants' power
30. Coordinated Plan on Artificial Intelligence 2021 Review | Shaping Europe's digital future
31. Parliaments negotiating position on the AI Act

32. Data Protection Directive - Wikipedia
33. General Data Protection Regulation - Wikipedia
34. What are the GDPR consent requirements? - GDPR.eu
35. GDPR EXPLAINED: The 6 Legal grounds for Processing Personal Data LAWFULLY
36. It's high-time for internet access to be recognised as a fundamental right – MEP Josianne Cutajar - The Malta Independent
37. Türkiye Doubles Down on Violations of Digital Privacy and Free Expression | Electronic Frontier Foundation
38. https://www.dlapiperdataprotection.com/index.html?t=online-privacy&c=TR&c2=
39. Country Insights | Human Development Reports
40. Japan-act-on-protection-of-personal-privacy-appi
41. https://blog.didomi.io/en/japan-data-protection-law-appi-everything-you-need-to-know
42. https://iclg.com/practice-areas/data-protection-laws-and-regulations/taiwan
43. Data Protection & Privacy 2023 - Taiwan | Global Practice Guides
44. Personal Data Protection Act - Article Content - Laws & Regulations Database of The Republic of China (Taiwan)
45. Yemen | Global Information Society Watch
46. Covid-19 and Data Privacy Challenges in Taiwan
47. Congo | DataGuidance
48. New press and internet regulations in the Democratic Republic of the Congo | Digital Watch Observatory
49. Mali | Fact Sheet | Data Protection Africa
50. Kazakhstan - Data Protection Overview | Guidance Note
51. Exploring Privacy use cases in Ghana. | by Igboanugo Chinelo Clementina | Medium
52. New Zealand | DataGuidance
53. A new Era for Data Protection in Switzerland – Are you ready? | EY
54. Ready for the new Swiss data protection law? Implications for organizations outside Switzerland
55. Syria Cyber Profile
56. Human rights index - Our World in Data
57. NCSI :: Sudan
58. Octopus Cybercrime Community - Sudan