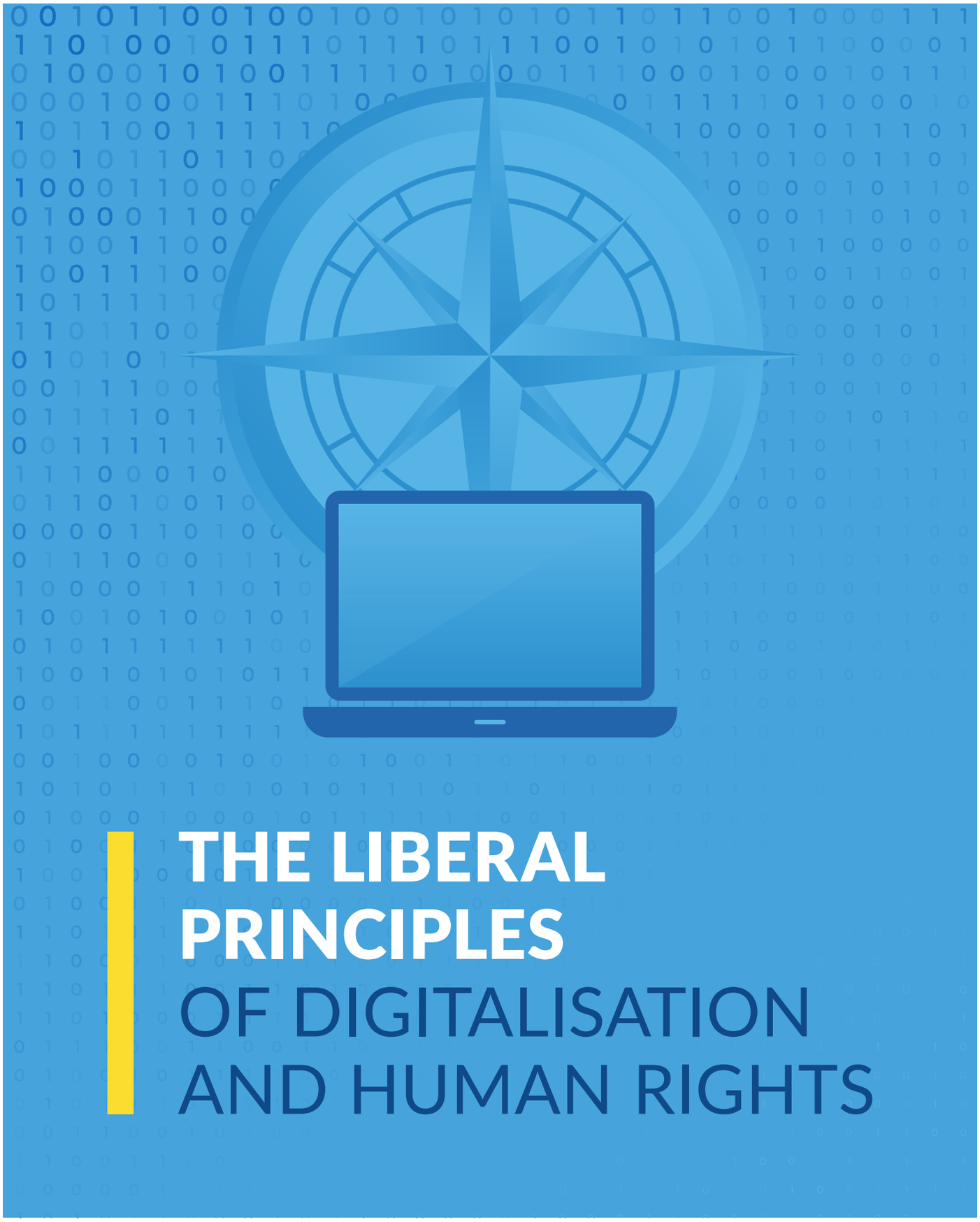


THE LIBERAL PRINCIPLES OF DIGITALISATION AND HUMAN RIGHTS

LIBERAL INTERNATIONAL

radikale B

TABLE OF CONTENTS

FOREWORD

When the Human Rights Committee elected in 2019 set up the priorities for the coming years, it was obvious we should deal with how digitalisation affects Human Rights. In a survey made, it could be noted that less than half of LI's member parties had any policy on human rights in the digital area. As the guiding principle of our work is to serve member parties, we thought this would be an area of the biggest value for the liberal audiences.

Naturally, there were so many examples of how digitalisation affects our societies: restrictions of access to the net, Cambridge Analytica and other forms of interference in elections, hate speech and fake news, and mass surveillance to name a few. And each month it seems there is something new coming up; for instance, the Pegasus spyware that seems to have been in use even in societies that surprise as.

If we would be a scientific organisation we would have to define what digitalisation is, but that has not been seen as necessary. We have been working with a broad definition taking into account the transformation from analogical to digital representation of information and the ubiquitous access to the internet and how both are changing our societies. Equally, we have kept an eye on the way Artificial Intelligence, AI and the huge masses of information treated by supercomputers spell out new challenges. However, some of the terms we use in the ten principles are explained in the glossary.

In a certain manner, it would be easy to just follow the first principle we have stated: Any human rights respected in the physical world must be equally respected in digital form.

But that is certainly not enough. We all understand that there needs to be new ways to protect our rights and freedoms in a world where so much more control is possible. And a very fundamental change is occurring at present, where data including information about every one of us and our behaviour has become one of the most valuable assets in society. Could it be phrased: Data is the raw material of the digital society? Therefore questions on data, ownership of data and data retention and how we can control information on us is a very central question.

For Liberals the right to privacy is central. Or as Irwin Cotler put is in a video, which explains one of the principles: privacy is the most comprehensive of rights and the right most valued by civilised people" quoting a sentence of a judge 100 years ago.

Actually, it has quite often been said that there are three models of data ownership in the world today: the Chinese where the society owns all data, the American where companies own much of the data and the "European" which tries to protect the privacy of persons and their data.

How were the principles elaborated?

A working group of the Human Rights Committee was set up - and I want to thank all the members of the WG and also MEP Karen Melchior, who came as an external expert. It was clear for the working group that we would not deal with the larger societal implications like questions relating to the regulation of the big tech companies or exactly how digitalisation should work in education and health care. There are many issues to continue to be discussed by us liberals, as we will at the Congress in Sofia. It is however essential to point out that access to the information society is also one of the first preconditions for a more equal world, where no one should be left out.

And in the midst of this work, the COVID-19 came, which meant that the work had to be done mostly in virtual workshops and webinars. In this regard, digitalisation helped us! But it also showed us what lockdowns and denial of access to the internet mean in authoritarian societies. Unfortunately, this trend continues in these times of war, with very severe repercussions for anyone showing dissent. During our work, we heard so many testimonies on how authorities try to use surveillance technologies to hinder civil society actors, but also how democracy activists use new technology to uncover electoral fraud or mobilize action.

When liberals elaborate policies, the discussions undertaken have been most valuable, as always. I think of the numerable webinars we have had; for instance with EU Commissioner Margrethe Vestager, responsible for making the EU fit for the Digital Age, UN Special Rapporteur on the freedom of opinion David Kaye, Nobel Laureate Maria Resa, former MEP Marietje Schaake - the expert of the EP on cyber issues, the digital minister of Taiwan Audrey Tang - to mention a few. I want to thank all who participated in the webinars and in our work, including recording the videos that explain the principles and are part of our campaign.

A big thank also goes to our human rights officers Mikaela Hellman and Irene Wang who distilled and initiated much of the discussion as well as Jason Fraser who helped in so many ways.

Finally: much of this work could not have been done without the support of the Danish member party Radikale Venstre (RV) which so generously has enabled us to have the campaign around the principles. A big thank Radikale Venstre.

Astrid Thors
Chair of LI Human Rights Committee

PS To get a good insight into the principles, please watch the ten videos and listen to the webinars, you will find them all on LI's homepage

THE LIBERAL PRINCIPLES OF DIGITALISATION AND HUMAN RIGHTS

We liberals,

Recognizing that the irreversible proliferation of digital technologies provides new avenues to exercise human rights and ingenuity for the betterment of society, including in denouncing electoral fraud,
Also recognizing that the same technologies are too often used to violate human rights and restrict freedoms to an unprecedented degree,

Recalling the Universal Declaration of Human Rights, European Commission Declaration on Digital Rights and Principles, and Manila Principles on Intermediary Liability,

Adopt these principles to guide liberal member parties in their policies and practices towards securing the protection of human rights and freedoms in the digital age:

1. Any human rights respected in the physical world must be equally respected in digital form.

2. Any legislation and technical tools put in place affecting human rights must be proportional and robust enough to **be acceptable under any government**, benevolent or not.

3. **Access to information and communications technology** and the right to information should be **inclusive**, where no part of the world or group in society is left behind.

4. **Openly and persistently denounce and work against the use of internet shutdowns** as a hindrance for enjoyment of human rights such as access to information, freedom of expression, health, education, and work.

5. **Strengthen policies and work towards the development of a common framework to** combat cybercrime and breaches of privacy and personal data security, ensuring transparency and due process when fighting cybercrime.

6. **Resist the introduction of any kind of legislation on or undermining storage encryption**, which risks infringing on the rights to privacy and data protection.

7. **Oppose mass surveillance** and develop alternative instruments, policies, and approaches to prevent and combat crime without degrading the privacy and software security of the entire society and every human being.

8. The transparency, accountability, and comprehensibility of tech companies and governments for their **use of data and data retention** must be increased, also ensuring that individuals know when their data is being collected and what it will be used for.

9. Transparency, accountability, and comprehensibility in the use of **artificial intelligence and emerging and disruptive technologies** must be ensured, to clarify chains of responsibility and ensure traceability in decision-making, and to allow societal oversight of the algorithms that have a significant impact on the lives of citizens.

10. Legislation on content moderation, aimed at managing hate speech, disinformation, or other malicious content online, **must not arbitrarily restrict the freedom of speech** or encourage private companies to pre-emptively censor content.

Glossary

Artificial intelligence: The development of computers able to engage in human-like thought processes and problem-solving such as learning, reasoning, and self-correction.

Disinformation: A form of propaganda involving the dissemination of false information with the deliberate intent to deceive or mislead.

Emerging and disruptive technologies (EDTs): Technological innovations such as artificial intelligence (AI), autonomous weapons systems, big data, biotechnologies, robotics, blockchain, and quantum technologies that are expected to have a disruptive impact on business, society, and national defense.

Encryption: A means of securing digital data, which can only be decrypted by the user with the encryption key. The encryption process translates information using an algorithm that makes the original information unreadable.

Hate speech: Public speech that expresses hate or encourages violence towards a person or group based on something such as race, religion, sex, or sexual orientation.

Internet shutdown: The intentional disruption of Internet-based communications, rendering them inaccessible or effectively unavailable, for a specific population, location, or mode of access, often to exert control over the flow of information especially during times of crisis, as a form of censorship and preventing access to information.

Mass surveillance: Indiscriminate monitoring, collection, analysis, use, retention, and storage of information and data of large or infinite numbers of people.

Proportional: If an action, law, or restriction impinges upon human rights, the need for the action, law, or restriction is justified by an overriding reason relating to the public interest and the objective pursued cannot be attained by means of a less restrictive measure.

Robust: Strong, powerful, and able to withstand challenge.

Storage encryption: The use of encryption for data both in transit and on storage media. Data is encrypted while it passes to storage devices, such as individual hard disks, tape drives, or the libraries and arrays that contain them.

Transparent: The concept of disclosing as much information as possible to users regarding how their personal information is handled. To achieve transparency, businesses and websites must give their users easy-to-understand, comprehensive information, as well as notification when information is updated. (GPDR, CCPA, CalOPPA)

ON ENCRYPTION: LIBERAL PRINCIPLES OF DIGITALISATION AND HUMAN RIGHTS

Written by Mallory Knodel

Principle 6: **Resist the introduction of any kind of legislation on or undermining storage encryption**, which risks infringing on the rights to privacy and data protection.

Encrypted architectures are designed to conceal user data from the central service provider, thereby promoting user agency. The strong privacy and confidentiality guarantees of encrypted systems are more important than ever in the digital age. Encryption protects the human rights to privacy and security, as well as free expression online according to former UN Special Rapporteur David Kaye.

While the processing of personal data has been regulated since the early days of the internet, contemporary data protection principles are easily fulfilled with ubiquitous implementation of strong encryption, yet encryption is still framed as "posing challenges" for policy makers, specifically in the context of policing and national security. To unpack the risks of undermining encryption, it's important to first understand encrypted systems through formal definitions as well as their features and characteristics.

Encryption and encrypted systems
To encrypt data, a system uses a secret key to output ciphertext. Only the secret key can decrypt the ciphertext back into readable plaintext. The applications of cryptography in wide use today secure data, and secure the communication of data between people as well as between computers. There are essentially three types of encryption schemes that formally describe how data is encrypted when it is in transit, at rest and end-to-end.

Encryption in transit means that encryption is deployed to protect data while it is being communicated over a network. Data is encrypted at one endpoint of the communication channel and decrypted at the other end. Example websites.

Encryption at rest refers to the use of encryption to protect data while it is stored. Data is encrypted right before it is stored and decrypted right before it is used. Example cloud storage. Who has the key.

End-to-end encryption (E2EE) protects user data at all times, during transit and while at rest. Data is encrypted on the user's device using a key that only the user knows. Because the user is the only one with knowledge of the key, its data is protected along every component of the system and against any potential attacker. A critical component in this type of encryption is the end-to-end principle - extending encryption between two end-points in the communication system, i.e., the sender and receiver (cite Mallory's IETF paper). A system, service or app is end-to-end encrypted if the keys used to encrypt and decrypt data are known only to the senders and the (designated) recipients of this data.

In addition to these formal definitions, encrypted systems can be described by their features. Authenticity, accountability, confidentiality and integrity of data can be achieved with various properties of encrypted systems.

Features of encrypted systems
Authenticity. A system provides communications authentication if the sender and/or recipient(s) agree on each other's identities and the contents of their communications.

Confidentiality. A system provides message confidentiality if only the sender and intended recipient(s) can read the plaintext of the communication, i.e. a message is encrypted by the sender such that only the intended recipient(s) can decrypt it, or a webpage sent with transport encryption can only be viewed by the user who requested it. Encryption cannot guarantee whether or not the recipient(s) or sender (such as a central web server) discloses through other means aspects of the communication.

Integrity. A system provides communications integrity when it guarantees that data that have been modified in transit can be detected reliably, or conversely that a recipient is assured that data cannot be undetectably modified in any way.

Accountability. Sender Binding is a desirable feature of encryption that prevents the receiver from being able to frame the sender for content that they did not send. A similar feature exists for Receiver Binding. Together, those features effectively comprise an unforgeability property of encrypted data.

Deniability. Along with authenticity, deniability is a property sometimes present in encrypted systems that ensures that in group chat environments if the content of a message is exposed that the other members of the group chat cannot conspire to falsely verify a reported message.

Forward secrecy. Forward secrecy is a security property in encrypted systems that prevents the decryption of data that was encrypted before an endpoint key is compromised. Conversely, post-compromise security guarantees a way to recover from an endpoint key compromise.
In practice e2ee is used in a number of ways, all of which have attracted the concern of law-enforcement and attention of regulators. From cloud storage to messaging to VPNs (virtual private networks) there are several policy level threats that weaken encrypted systems directly or erode the guarantees of these features.

Policy threats to encryption
There are persistent risks to end users through policy measures that seek to make encryption difficult to obtain, weaken encrypted systems and associated properties, or criminalise it including compelling decryption in criminal cases.

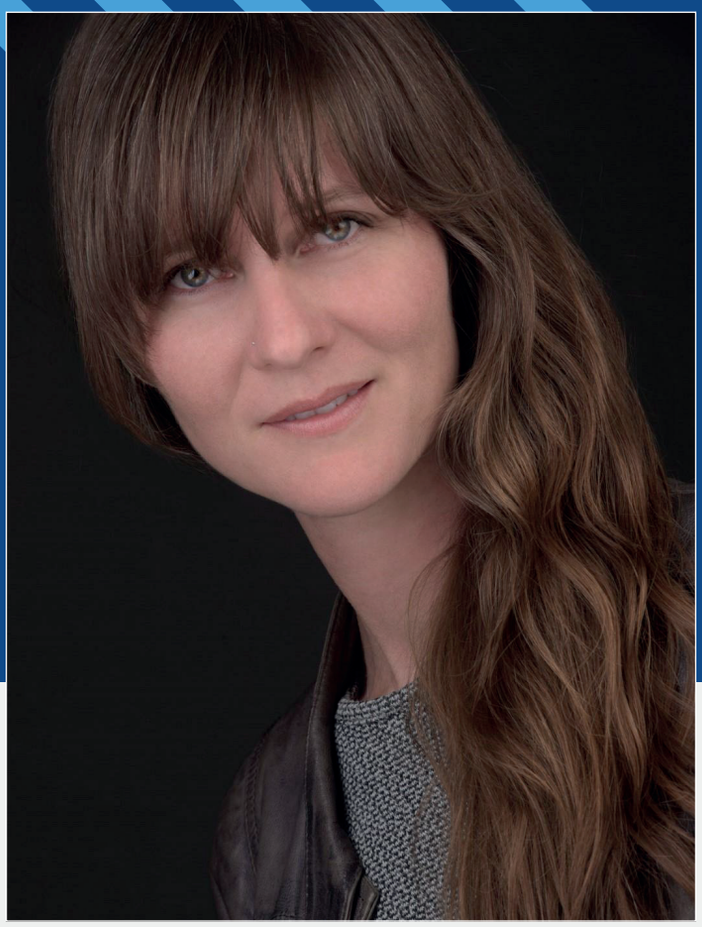
Making strong encryption difficult to obtain or employ is often done in more authoritarian policy environments through import/export controls, undue licencing, or policies that define maximum or minimum key lengths.

Given the ubiquity of transport encryption, criminalising the use of encryption is now a rare policy approach, however the use of end-to-end encrypted messaging has led to bans, network shutdowns, and arrests, leading to egregious human rights abuse by the authoritarian regimes where this approach has been taken. Similarly there are grave civil liberties implications for compelling decryption in criminal cases as a form of self incrimination.

Lawful intercept policies are by far the most risky to human rights in the current regulatory climate. Nearly all proposals for lawful interception would require a disproportionate response from service providers to modify their systems to trace user behaviour, collect and store user data, scan images and text, or even aid in identifying victims of crimes.

Beyond policies that directly threaten strong encryption, there are other regulations that nonetheless have implications for encrypted systems. Trust and safety guidelines might ask platforms to collect enhanced metadata about or otherwise moderate any content that supports terorrism or threatens child safety, but in a way that ultimately would be incompatible with the privacy and confidentiality promises of both at-rest and end-to-end encrypted systems. The same is true for regulations targeting the unauthorised spread of intellectual property.

Human rights are threatened by legislation that requires data retention for any internet services, but in particular it erodes the assurances provided by end-to-end encrypted services. Any legislation that directly undermines storage encryption in platforms or devices or compelled decryption are grave threats to human rights and civil liberties. These policies risk infringing on the rights to privacy and data protection, in addition to other rights enjoyed both online and offline in the digital age.



Mallory Knodel is the CTO at the Center for Democracy & Technology in Washington, DC. She is a member of the Internet Architecture Board, the co-chair of the Human Rights and Protocol Considerations research group of the Internet Research Task Force, co-chair of the Stay Home Meet Only Online working group of the IETF and an advisor to the Freedom Online Coalition. Mallory takes a human rights, people-centred approach to technology implementation and cybersecurity policy advocacy. Originally from the US, she has worked with grassroots organisations around the world. She has used free software throughout her professional career and considers herself a public interest technologist. She holds a BS in Physics and Mathematics and an MA in Science Education.

ON DATA RETENTION: LIBERAL PRINCIPLES OF DIGITALISATION AND HUMAN RIGHTS

Written by Prachi Mishra

Principle 8. The transparency, accountability, and comprehensibility of tech companies and governments for their use of data and data retention must be increased, also ensuring that individuals know when their data is being collected and what it will be used for.

Introduction

The world stands on the cusp of the 4th Industrial Revolution and data will spearhead this paradigm shift. Emerging technologies of today, like Machine Learning, Artificial Intelligence, Internet of Things et al, all rely on data and its synthesis. As the world becomes more interconnected and the ease of access to the internet increases, data collection and collation has also grown exponentially. In the last few decades, data has become the cornerstone of trade, commerce, political decision making and lawmaking, technological evolution, and all other facets of our existence. For instance, large firms rely on millions of datasets to optimise their supply chains. Manufacturing firms use data analytics to improve product design, its quality, and decide quantities of product manufacturing. In fact, all companies, irrespective of their size and functioning, use data to maximise profits and improve their services. Government and its agencies also make use of data of their citizens to make delivery of public service and goods more efficient, to cut losses (like losses incurred in transmission of electricity), reduce corruption, and streamline their political agenda with the will of the people.

In this backdrop, the importance of ethical use of data becomes quintessential. With greater penetration of mobile applications and consumption of data, the number of cyber attacks have also witnessed a steep rise in the last few years. Also, there are several ethical dilemmas that grip policy makers around the world on issues like data ownership vs. data processing, the use sensitive personal information for commercial activities, incorporating consent of the user in data collection, ethical use of data vs. profit making, seeking active participation of the users when it comes data-related decision making, and enforcing a blanket of data governance rules on different data use cases. These global discourses have shifted the onus of data collection and its protection on organisations and it is up to them to figure out the best ways they can do the needful. In simpler terms, data collecting organisations are now faced with an additional responsibility: to ensure that the data collected is safe, secured, and protected against any malign use.

Hence, there is a pressing need to define certain key concepts, like, accountability, transparency, and comprehensibility for both, governments and private players to ensure ethical accords for data collection, usage, and dissemination are set in place.

Key concepts

Transparency: To foster trust and loyalty among the users, it is important that private players and governments collect, store, and share their information in a transparent manner. This implies that personal information and sensitive data should not be exploited or compromised for financial profits or gains of any nature. They must ensure that personalisation of services, which is one big reason for personal data collection, is in accordance with the ethos of data transparency. For this purpose, several governments have enacted laws and have put compliances in place for their organisations. For instance, Europe's General Data Protection Regulation (GDPR) and California's Consumer Privacy Act (CCPA), have made it mandatory for data collection entities to follow the principles of transparency.

Accountability: Accountability calls for organisations to make reasoned, responsible, and legitimate decisions about the use of data whether or not there is consent from the consumer. Organisations often need to comply with certain external laws (like the GDPR) or criteria for ethical use of collected data and to ensure fair compliance, they should frame internal policies, frameworks, and mechanisms that result in data protection and credible management of collected data.

Comprehensibility: Techniques and methodologies used for data synthesis should ultimately deliver key insights and patterns from collected data. The end goal of data processing is to assist in decision making and for this purpose, patterns and insights derived should be comprehensible and easy to understand for the layperson. Since decision makers in private companies and policy makers in the government need not necessarily be experts in data science, it is quintessential for organisations to ensure that outcomes of data processing are straightforward. If they are unable to understand what patterns mean and represent, they will not be able to use them. Hence, comprehensibility or the ability of data processing techniques (like algorithms) to deliver insights which are understandable by humans is critical.

Data retention: Data retention policy of an organisation is reflective of what data it stores, where it is stored and for how long it is stored. It also governs how an organisation disposes off the collected data in case it is no longer required. As companies and governments become more data-driven, it becomes their responsibility to keep the users informed of their data retention policies and to keep them abreast of any changes in the policy. As discussed earlier, key tenets like transparency, accountability, and comprehensibility form the basis of data retention policies for any organisation. These aid not just in regulatory compliance but also uphold data privacy and protection.

Consent of the owner for data usage and other purposes: While organisations can collect data from users for business growth or improved delivery of a product or a service, they must ensure that the user is consulted before his/her data is utilised. Asking the user for their permission to use their data before processing can also be helpful in trust building. Since consent is at the core of many issues around data protection, privacy, and data security, organisations must innovate mechanisms to ensure that data processing, storage, and dissemination is carried out only after the wilful agreement of the user.

Concluding remarks

With growing dependence of organisations on data, the trust deficit between the data collecting agencies and the consumer has increased. All major key digital debates in the world also echo this widening trust gap. Since a major proportion of the users are not aware of the usage of their data, it is critical that organisations take the first step in ensuring privacy is not compromised and personal information of people is not misused. Hence, it is for these organisations, whether government or privately held, to incorporate the tenets of transparency, accountability, and comprehensibility in their internal policies.

Prachi Mishra is a Young Leaders in Tech Policy Fellow at the University of Chicago Harris School of Public Policy. Through her fellowship, she is associated with the Delhi-based Observer Research Foundation on their Quantum Meta-Ethics project. Apart from quantum, she also reads & writes about tech sovereignty, digital democracy, human rights in the digital age, meta-ethics, and psychological implications of emerging technologies.

She holds an undergraduate degree in Computer Science and Engineering and a postgraduate in Policy, Design, and Management from the Indian School of Public Policy.

Published By:
Liberal International

With the support of:
Radikale Venstre
Christiansborg Slotsplads 1
1240 København K
internationalofficer@radikale.dk

Edited by: Liberal International

1 Whitehall Place
London
SW1A 2HD
United Kingdom

office@liberal-international.org

WWW.LIBERAL-INTERNATIONAL.ORG