SHERPA
BRIEFING

SIS and Privacy and Data Protection

The SHERPA project has analysed privacy and data protection primarily in the EU, focussing on the implications of technological developments on personal data. This briefing paper addresses the challenges stemming from technological advancements for data protection and consumer privacy, as well as ways to tackle such issues in the EU.

THE CASE/SCENARIO

Privacy can be broadly defined as a person's right to control access to his or her personal information, while personal data have been defined as any information that relates to an identified or identifiable living individual. Technological developments, such as social media and voice controlled personal assistants, present novel challenges to the understanding of privacy and data protection. AI provides an innovative way of collecting, analysing, and combining data on a large scale and quickly. Given the automated nature of these systems however, there is limited supervision and/or surveillance. Therefore, how can one establish harmonised protection across frontiers and guard against data manipulation? Has the European Union responded adequately to the modern challenges of the globalised market?

ETHICAL ISSUES

- The approach taken by national authorities and governments as part of their SIS governance and urban management strategies may pose a threat to privacy, security, accuracy, and data ownership. Given the overlap between public and private interests, there cannot be a single governmental line of application of SIS, as illustrated by the Sherpa Case Study on Sustainable Development for smart cities and public spaces.
- Data breaches can lead to the exploitation and misuse of personal data including the identification of a person's background, gender, social connections, health, or other personal characteristics, as evidenced by Cambridge Analytica.
- The privacy of consumers can be infringed using technology such as Google Assistant and Siri which can record more than what was expected by the consumer.
- Data can be stored across various locations. There ought to be a system addressing explicit requests for the deletion of data and the enforcement of the right to be forgotten.

This project has received funding from the European Union's Horizon 2020 research and innovation programme, under grant agreement No 786641.

LEGAL ASPECTS

- The right to privacy has been enshrined under Article 8 of the ECHR and Article 7 of the EU Charter of Fundamental Rights stating that the right to privacy is a fundamental human right. The development of the right to privacy was associated with innovation and technology, leading to the creation of the express right to data protection under Article 8 of the EU Charter of Fundamental Rights.
- Since 2018 the EU General Data Protection Regulation (GDPR) has also entered into force, reshaping the handling of data across many sectors such as healthcare or banking. Data minimisation is one of the core principles under the GDPR, as enshrined under Article 5, where only "adequate, relevant and limited" personal data can be processed. Therefore, there ought to be a transparent and delimited use of data. Article 6 provides the grounds on which data processing will be lawful such as the acquisition of prior informed consent.
- The right to be forgotten was developed by the EU Court of Justice, and subsequently enshrined in the GDPR. It enables individuals to request the deletion of their personal data.
- In addition to the Digital Single Market Strategy, the European Commission has provided AI ethics guidance which emphasises the importance of privacy and data protection at "all stages of the life cycle of the AI system" including the information provided by the user and generated about the user.

LESSONS LEARNED

Privacy is a fundamental right which ought to be protected given the sensitivity of personal data. The EU institutions, Member States and interest groups have taken significant steps to reinforce protection and strengthen pre-existing legal frameworks. The GDPR is a step in the right direction. Nevertheless, rapidly developing technologies require constant legal evolution and reassessment, so as to adequately protect privacy and data protection as dynamic rights. Case law at the European and national level as well as soft law instruments are also essential to accommodate the modern labour market but also widen the spectrum of public discourse on the right to privacy and data protection.

This project has received funding from the European Union's Horizon 2020 research and innovation programme, under grant agreement No 786641.