DiPLO
www.diplomacy.edu

Geneva Internet Platform

DATA TALKS JUNE 2018: *DATA DEPENDENCY AND EXPLOITATION*

The management and use of personal data by international organisations and other actors raises important ethical concerns, especially when data is collected from and/or about vulnerable populations. The session focused on the risks related to the challenges of the collection and use of data in humanitarian contexts, the collection and use of children's data, and general challenges related to data protection and possible misuse in using technology to reinforce security. Can consent in humanitarian operations be considered 'informed' if there is no opt-out? When personal information is given up without immediate feedback or solutions provided, how to avoid perceptions of exploitation? In addition, how to collect and manage children's and young adults' data? Which impact has technology used to reinforce security on data protection and fundamental rights?

Management of refugees' data

Shelley Gornall, Senior Information Management Officer at the United Nations High Commissioner for Refugees (UNHCR), presented on the paradoxical need to gather an increasing amount of personally identifiable data while making data more open than ever before, particularly in humanitarian conflict situations.

She explained that UNHCR is trying to further empower refugees by providing them a "digital identity," which will allow them access to information and services online. Currently, the amount of data required to run an operation is growing exponentially for many reasons. For example, technological advancements in data collection make it easy, fast, the ability to share data quickly, through APIs and HXL and other means to transfer machine-readable data between organizations.

This increase in demand for data is matched with ever-increasing tension between the protection concerns and the Open Data Movement, which generates an expectation that not only analytical products but microdata will be shared. These practices raise several ethical and practical problems, regarding, for instance, how "informed consent" is communicated, how it is updated when additional uses are foreseen for the data that were not anticipated upon collection and, lastly, concerns on how we can anonymize data efficiently thus avoiding re-identification of sensitive information.

She stated that collecting personally identifiable information is necessary and unavoidable, and the best way to mitigate the risk is to prevent data breaches from happening in the first place. Tracing back the cause of a data breach is difficult; even realizing one has occurred is challenging; tracing the impact of a breach is even more difficult.

In 2015, UNHCR introduced its Policy on the Protection of Personal Data for Persons of Concern to UNHCR. The policy established a Data Controller in every operation (the Representative) and a Global level Data Protection Officer. It stipulates that persons of concern are "Data Subjects" who own and control their personal information and that data processing must be "legitimate and fair." The standards used in this policy are comparable to the European Union's General Data Protection Regulation (GDPR), which doesn't legally apply to UNHCR due to UN immunity, but UNHCR has aligned itself to it to a good extent. UNHCR would like all its partners to have a similar policy.

Shelley Gornall also considered that aside from personally identifiable data, collecting any protection data is a risky business and UNHCR's data collectors have suffered retribution for it. Thus it is important for the organization to protect data collectors' identities, particularly in protection-hostile environments.

Data collection impacts security and humanitarian space. Humanitarian organizations have a responsibility to anticipate the impact of data collection and publication, on not only their own organizations but others, including smaller NGOs.

She concluded by adding that further to UNHCR initiatives, there are several interagency initiatives addressing these ethical issues, including the Protection Information Management project and the Grand Bargain Commitments on Coordinated Needs Assessment.

Children's Privacy Online

Patrick Geary, Corporate Social Responsibility Specialist at the United Nations Children Fund (UNICEF) discussed the topic of children's privacy online. UNICEF's focus on the online protection of children's data has changed from an approach focused on the prevention of violence, exploitation and abuse of children to a more holistic one comprising also children's right to access to the Internet. The amount of data collected about children, before they turn 18 is impressive as it ranges from data collected through pregnancy monitoring to Internet of Things' (IoT) and smart toys. More importantly, it is impossible to clearly understand the current and future impact of such collected data. The digital world threatens children's online experience in several ways: privacy concerns represent just one of the topics of the current discussion on the determination of children rights online.

UNICEF works with an industry-based working group with representatives from Google, Facebook and IoT devices companies in order to create a rights framework. Geary stressed that a multi-stakeholder approach is essential to achieve this goal. In addition, the balance between the protection of children's rights and the limitation in the services that are offered is often missing: how to protect children's rights without infringing upon their right to access to the Internet? In this regard, a discussion started regarding the rights of future generations - an issue that is particularly of relevance if we consider the recent developments in Artificial intelligence (AI).

The issue becomes even more complicated if we look at the concept of informed consent given by children - especially because definitions of 'informed consent' differ depending on the legislation under consideration and the age of the child. For UNICEF, everyone under 18 years old is considered a child and treated as such. However, the notion of 'evolving capacity' is used to address the capacity of showing a different degree of consent according to the maturity of the child.

Challenges Related to Technology to Reinforce Security: Data Protection

Francesca Bosco, Programme Officer at the United Nations Interregional Crimes and Justice Research Institute (UNICRI), discussed the challenges faced by many organizations collecting massive amounts of data on beneficiaries, including personal identifying information (PII) for the purpose of better developing evidence-based solutions to drive social impact. She focused on risks of data mismanagement of vulnerable populations (e.g. children, youth, minorities, indigenous peoples, migrants, internally displaced persons, refugees, stateless persons, persons with disabilities, members of the LGBTI community, older persons, and women and girls exposed to multiple threats). She underlined that data protection is not just a matter of encryption but also of security policies in place. For example, many international organisations do not have adequate data protection policies, very few have threat models risks and security protocols in place while globally there is a lack of standards and monitoring. Thus, a primary concern is the need to reduce the risk of 'mismanagement', i.e. avoid practices that could lead information to be misused by mal-intentioned actors, potentially leading to physical harm and ill-treatment. Thus, the protection of data is crucial and despite the progresses made with the EU's GDPR, ICRC's Handbook on Data Protection in Humanitarian Action, and UNHCR's data protection policy, further steps have to be taken. In this regard, two of UNICRI's projects should be recalled: the Profiling Project on the identification and tracking of the challenges posed by technology to the fundamental right of privacy and data protection of citizens; and the current SIRIO Program on the promotion of knowledge and awareness on technology solutions to address emerging security risks. The Profiling Project focused mainly on automated profiling, i.e. the automated processing of data to develop predictive knowledge (namely profiles) that can be used as a basis for decision-making. The study found that there is a hiatus the design of a database and its implementation and use. For example, relevant databases are used for different purposes at the same time and there is a tendency to grant access to new authorities, usually unrelated to the original scope of the data collection. Consequently, data protection rights are often established on paper but not fully enforced in practice.

On the other hand, the SIRIO project aims at addressing emerging security risks through a three-step methodology. First, it analyses and identifies emerging security risks by realising a risk scenario which includes narratives, causes, consequences, impact and probability of a given incident. Second, it maps technology solutions to discuss how technology can concretely contribute to mitigate risks related to the scenarios. Third, it promotes the results of such risk scenario and related technological solutions. Successful examples of topics discussed are big data analytics to reinforce security, Identification of emerging security risks in biotechnology and opportunities and challenges of the blockchain.