Responsibly mining the “New Gold”

Geneva Policy Outlook

Jan 30, 20235 min

Digital Data is the “New Gold” that businesses collect, store and sell for great profits. But, how can we mine it responsibly and co-construct an effective oversight and governance system?

By Anne-Marie Buzatu

Digital Data is the gold of the 21st century. It is nearly impossible to browse a website, write an email, or use a mobile app without generating copious amounts of data. This data is, in turn, eagerly sucked up by online providers and sold to a variety of different customers for reasons more to less benign. This practice is concerning because, unlike gold or oil or other valuable commodities, data is not anonymous; rather, it is imprinted with our thoughts, habits and preferences. This digital footprint reveals the most personal aspects of our private lives, and our digital traces become the foundation for the digital economy. As the saying goes, “when using online offerings and you don’t know what the product is, then *you* are the product”.

Some individuals don’t worry much about this state of affairs and respond that they have “nothing to hide” and that they would like to use the "free" services. This rationale might work for individuals living in reasonably well-functioning democratic societies that feel assured about the safeguards to prevent the misuse of data, especially when it comes to

the violation of our basic human rights. However, such attitudes are problematic because data is being used to ends that most people are not aware of and beyond any serious oversight. For the last 75 years, human rights standards have helped to protect people's personal integrity. With a new "gold rush" well underway, it is high time to apply the same human rights standards within the digital space.

At one extreme, consider a series of reports by the *Times* in June and July 2022 about the "surveillance state" in China. In the city of Zhongshan, microphones are distributed along with video cameras to record audio and analyse conversations with voice recognition software and collect the voiceprints into a database. Another reportreveals that in Xinjiang, home to millions of Uyghurs, a contractor has built a database that can hold iris scans of up to 30 million individuals, and this same contractor is now building databases across other areas of the country. It goes on to say that the Chinese government is capturing and consolidating all of these data points with the overarching goal of building "a comprehensive profile for each citizen" and using mass surveillance to support its authoritarian rule. A BBC article reported on the use of a Covid-19 app by Chinese authorities to flag persons involved in protests; the persons were erroneously flagged as being Covid-positive, which subsequently prevented their free movement. This gives a completely new meaning to China's "Zero Covid" policy.

These realities appear like a modern-day Orwellian *1984,* and they are not just limited to China. Consider the revelation in the US that telecom companies are selling people's precise location coordinates generated by advertisements on their mobile phones. The *New York Times* reported in January 2021 that US military agencies were buying mobile phone location data from third-party brokers to trace past movements of users without judicial supervision. This is done even though a 2018 US Supreme Court ruling found that the US Constitution's protections against "unreasonable searches and seizures" required government officials to get a judicial warrant in order to obtain the same information directly from phone companies. Mobile phone companies routinely sell this information to third-party brokers, who then typically sell it to advertisers for marketing purposes. Because this information is freely available on the market, US military officials maintain that they should also be able to buy this information, even though it may be used for law enforcement purposes.

"In a sector where development and advances are primarily driven by commercial or military purposes, how can we safeguard human rights while realising the enormous educational, artistic and societal potentials of ICTs?"

This last example demonstrates an agency within a democratic government obtaining sensitive information, ostensibly in contravention of its laws, by purchasing it in the open market. Not only does this raise important red flags relating to governance, but it also begs the question of why this sensitive information is available for anyone with sufficient funds to purchase in the first place. How do we translate democratic notions of privacy and human rights more broadly to the marketplace of Information Communications Technologies (ICTs)? In a sector where development and advances are primarily driven by commercial or military purposes, how can we safeguard human rights while realising the enormous educational, artistic and societal potentials of ICTs?

The first point is a reality check: Regulatory processes are too slow to keep up with the pace of technological change. There have been some efforts to develop international standards for data and privacy protection, including at the Organisation for Economic Cooperation and Development (OECD), as well as by the Asia Pacific Economic Cooperation (APEC), which has developed the APEC Cross Border Privacy Rules System (CBPR). One of the most developed frameworks is the EU's 2018 General Data Protection Regulation (GDPR), which is a framework for data protection and privacy that regulates the collection, use and processing of personal data of individuals within the EU, with substantial financial penalties for organisations that violate the GDPR. However, since most individuals accept without reviewing/opting out of the numerous categories in which our data is collected, the result is largely the same, even for individuals living in the EU. Owing to this disparity, efforts should focus on setting more robust human-rights protecting standards for the kinds of information that are allowed to be collected and stored in the first place, with or without the user's approval, as well as the applications of oversight mechanisms that work in cyberspace.

"Instead of forcing "cyber" into ill-fitting existing public regulatory structures and silos, efforts should focus on the question of what kind of cyberspace the world wants to create — one that is safe, protects our private lives and can empower people in their daily activities."

In order to advance the application of human rights standards in 2023, a first priority action is a stocktaking of existing frameworks that regulate the digital economy and where they fall short with respect to human rights standards. Such an effort should also explore how to update existing frameworks so they are more effective in complying with basic human rights norms. The second priority action for 2023 is to start building a coalition that can develop and drive the oversight mechanisms. As "cyberspace" is a space co-created by commercial actors, academic and technical experts, members of civil society, as well as of governments, it is important to designate specific roles and responsibilities as part of this oversight architecture. Instead of forcing "cyber" into ill-fitting existing public regulatory structures and silos, efforts should focus on the question of what kind of cyberspace the world wants to create — one that is safe, protects our private lives and can empower people in their daily activities. In this process, there is a responsibility for everyone, but this responsibility has to be clearly articulated for each actor within this multistakeholder community.

With no time to lose, 2023 should be the year of action to apply human rights standards to the digital economy. There is much to learn from the business and human rights community and other sources of the relevant expertise of International Geneva and beyond. Those willing to lead should step forward to co-construct an effective multi-stakeholder oversight and governance system for the digital economy. There is no need to wait to develop measures of responsible mining that apply to the "new gold" of data so that the digital economy uplifts, rather than represses, the human experience.

About the Author

Anne-Marie Buzatu is the Executive Directorof ICT4Peace Foundation. An international lawyer, she also worked for several years in the information technology sector as a web developer and database administrator. This enables her to translate between policymakers and technology specialists and identify pragmatic and effective cybersecurity policy and governance approaches.

Disclaimer

The opinions expressed in this publication are those of the authors. They do not purport to reflect the opinions or views of the Geneva Policy Outlook or its partner organisations.