EXTRACT FROM THE ASTANA CLUB TOP 10 RISKS FOR EURASIA 2021

ASTANA CLUB

RISK 9

DIGITAL TOTALITARIANISM

Source: Shutterstock
Author: Mopic

DIGITAL TOTALITARIANISM

9 RISK

The pandemic has demonstrated convincingly the fact that technologies designed to facilitate communication are actively used to massively and uncontrollably collect personal information from the population.

As a result of the colossal concentration of personal data in the hands of global players in the information technology market, “digital control” over the lives of citizens becomes total, actively invading the jurisdictions of nation states around the world.

In 2021, the countries of Eurasia will face a difficult choice of format and model for their further digital transformation from complete market freedom in the digital sphere to a more rigid and unambiguous definition of the boundaries of digital sovereignty.

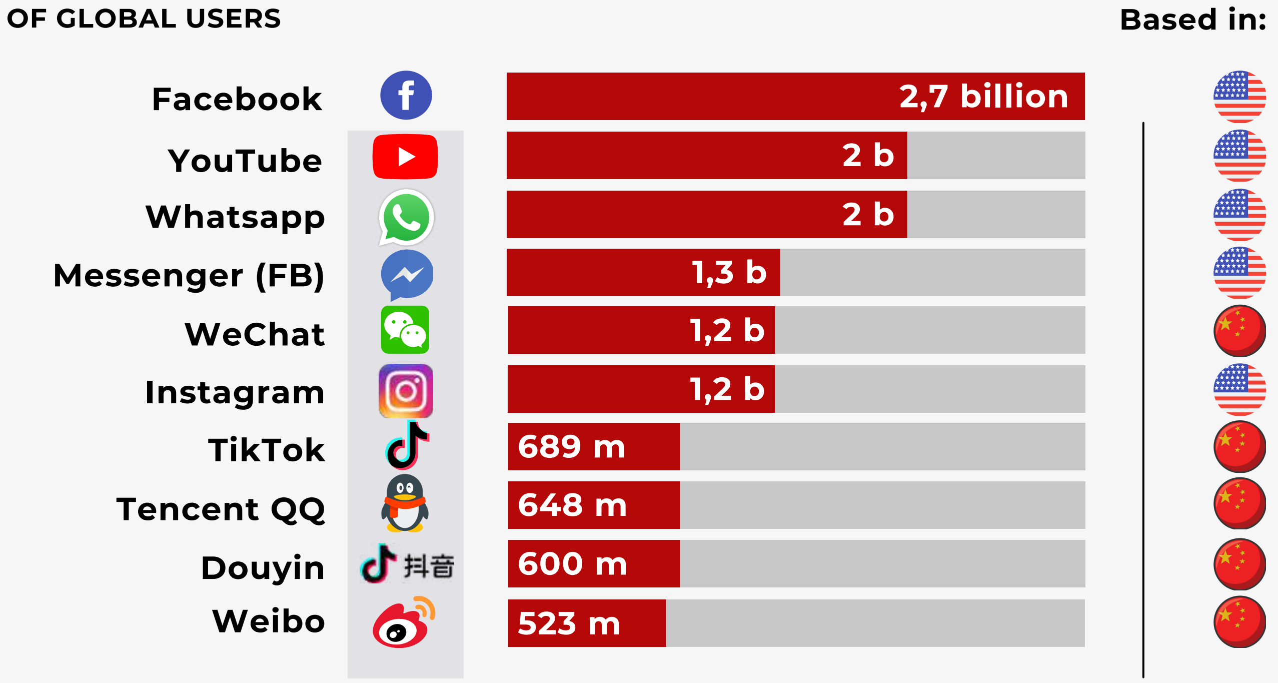
"BRAVE NEW WORLD"

The pandemic was the starting point for the finalization of the Data Economy and Data Society. At the center of the new format of the economic structure and business models is the digitized personality.

Personal data is becoming the main economic category: the "oil of the XXI century." In the new digital society, the main task is to establish control over information by analogy with managing the flows of world finance and natural resources.

The largest players in the digital information market, such as Facebook, Apple, Google, Tencent and others, accumulate colossal streams of metadata on their platforms, simultaneously exerting a large-scale impact on social, cultural and even political processes in societies around the world.

TOP-10 SOCIAL MEDIA PLATFORMS RANKED BY NUMBER OF GLOBAL USERS



Source: Data Reportal

A fivefold increase in the volume of data generated by government services, companies and citizens by 2025 will allow the owners of information "banks" of data to obtain an unprecedented level of access to a person's private life in history.

The monopoly control of IT corporations over the activities of leading social networks already allows them, at their own discretion, to determine permissible content, block unwanted information and shape public opinion. Respect for the right to free speech in the Internet age is no longer guaranteed. Examples of blocking accounts and deleting posts for political reasons, even by heads of state, make ordinary users dependent on the ideological attitudes and preferences of commercial companies. If states do not find tools to influence IT giants, the prospect of maintaining "digital sovereignty" for each individual country will tend to zero.

PERSONALITY TRANSFORMATION

The global process of human digitization has successfully passed the stage of creating a "digital avatar" and moved on to the stage of filling the "digital profile".

In addition to the primary data on the place of birth and residence, marital status and property, the profile is "overgrown" with information from the credit dossier, police databases and video surveillance systems, information about the nature of relationships with relatives and neighbors, participation in charity and other events.

In fact, citizens are no longer required to consent to the collection of information, which is non-stop using Wi-Fi networks, video cameras with face recognition technologies, biometric scanners, QR codes, etc.

Steve Durbin,
Managing Director
of the Information
Security Forum

Highly connected ecosystems of digital devices will enable the harvest, repurpose and sale of sensitive behavioural data about individuals without their consent. There are also a growing number of sectors that will see an increased dependency on behavioural analytics, including finance, healthcare and education.

With the introduction of 5G technologies and the expansion of the range of Artificial Intelligence (AI) applications, the profile of any person will be integrated with data from the Internet of Things, report cards in an educational institution, a medical record, etc.

"Splicing" a person with digital gadgets leads to the fact that now computer algorithms make decisions for the user themselves. At the same time, the recommendatory nature of the proposals can easily be replaced by a mandatory one.

The mechanisms of "compulsory medicine" are already being worked out as part of the fight against the spread of COVID-19. China's Health Code app, European Gateway, and Apple's and Google's apps that track coronavirus transmission highlight the potential for digital surveillance for medical purposes. As a result, the ever-increasing access to personal information on the part of IT giants and individual states allows them to launch large-scale behavioral programming processes.

The example of China, which has created a social rating system for its population, clearly demonstrates the possibilities of new digital technologies

This social experiment on behavioral programming of more than a billion inhabitants of the world's largest country by population is unprecedented in scale and nature.

Vladimir Yakunin,
Head of the Department of State Policy, Faculty of Political Science, Lomonosov Moscow State University

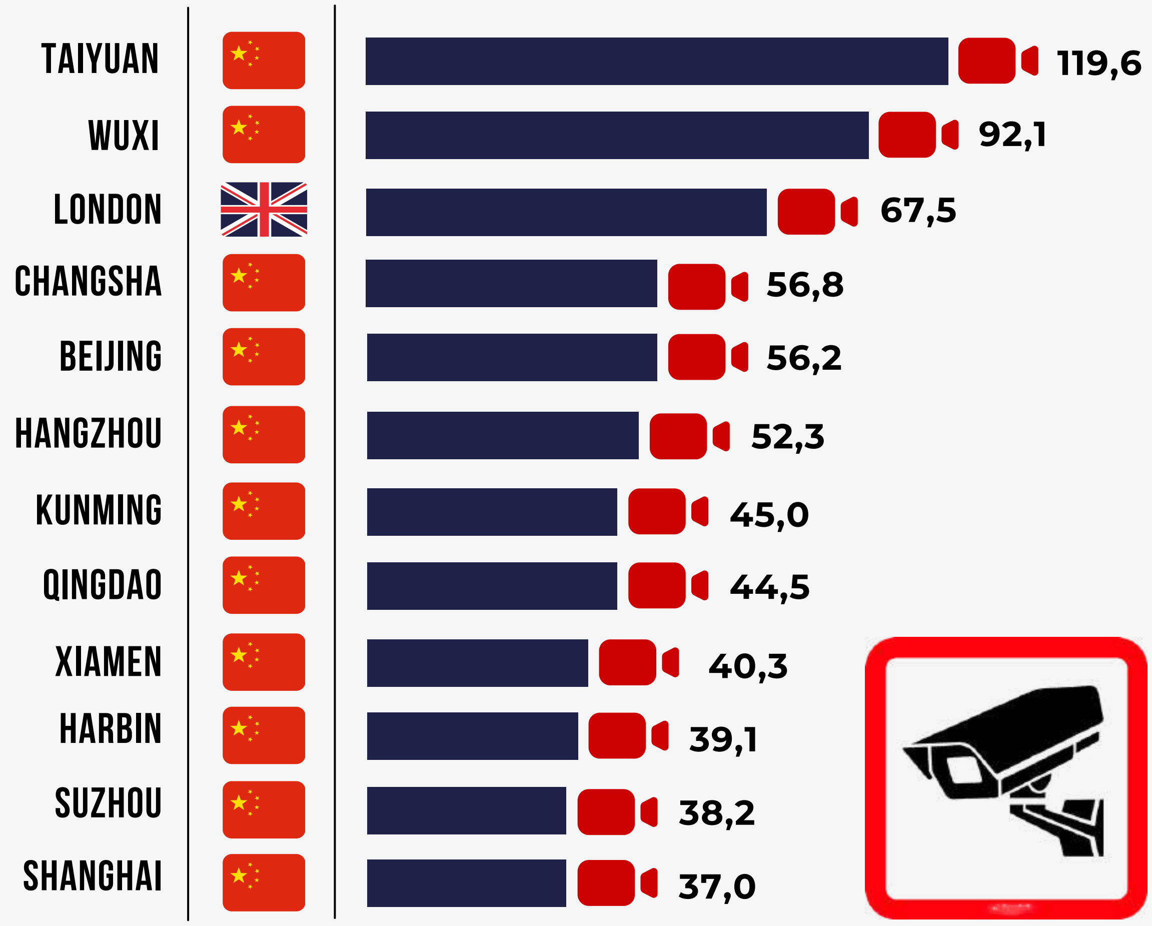
Signs of total digital control are already present in most countries where the Internet and social networks are widespread. The key issue is to regulate these technologies, to ensure their safety. Traditionally, this has been the responsibility of the state.

The formation of an "improved" citizen who accepts the new rules of the game in exchange for comfort and various preferences in social life establishes a person's total information transparency in front of corporations that control information flows.

BIG BROTHER IS WATCHING

The situation with the COVID-19 pandemic has rapidly increased the pace of adoption of digital behavioral monitoring technologies around the world. The introduction of 5G technology and the emergence of super-speeds for data transfer are giving an unprecedented boost to video analytics.

CCTV: THE MOST SURVEILLED CITIES IN THE WORLD
Cities with the most surveillance cameras per 1000 inhabitants in 2020



Source: Comparitech

Thus, the global video surveillance market will have increased by $36 billion by 2024 with an average annual growth of about 12%.

In Europe and North America alone, camera numbers are projected to grow by 18% annually, resulting in 420 million camera installations by 2024. Already today, about 200 million cameras have been installed in totally digitalized China, which makes it possible to make massive use of face recognition technology. Today, 18 of the 20 most “watched” cities in the world are located in the PRC.

Modern smartphones also offer unprecedented opportunities for collecting information about their users and the social environment around them. According to statistics provided by Exodus Privacy, almost every Android application contains at least one tracker, which is responsible for advertising, authorization and analytics.

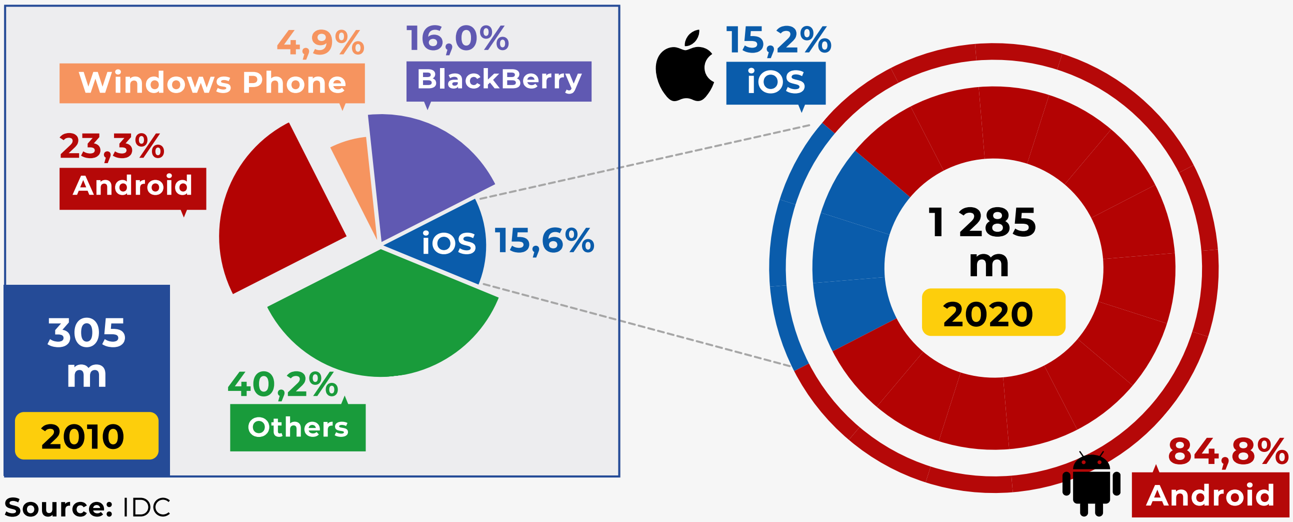
At the same time, the technical "stuffing" of the digital platforms used allows data to be transferred to servers and cloud storage services outside state borders, which raises serious questions about ensuring national information security. In fact, we are talking about the fact that the ownership of digital technologies guarantees control over those who use these technologies. As a result, the rapidly emerging global digital space presupposes the integration of states into the system of the new business model of IT giants, and not vice versa.

FORECASTS

The pace of global digital transformation in 2021 and the coming years will accelerate exponentially across the entire world. The pandemic has only become a catalyst for a long-standing process of creating a digital system for monitoring human behavior on a global scale.

The race for biometric and other personal data will intensify the widespread intervention of the world's leading players in the digital industry.

THE SMARTPHONE DUOPOLY
Worldwide smartphone market share by operating system



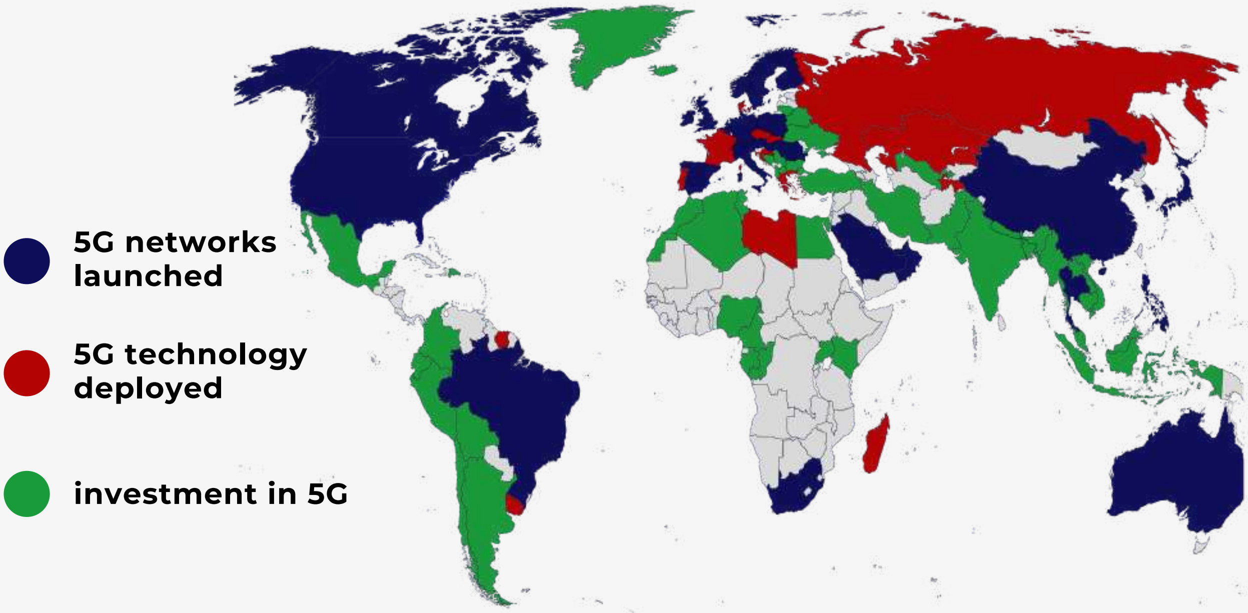
Source: IDC

Further use of the accumulated volume of personal data turns into a powerful tool for behavioral engineering of the population by the leading global IT monopolists. In these conditions, the process of merging the interests of technological giants with the interests and needs of states of their main jurisdiction will continue, including in solving foreign policy problems, economic and ideological expansion. Already today, there are active attempts to use popular social networks and instant messengers to influence social, cultural and political processes in a number of countries around the world.

However, against this background, the response to the strengthening of national "digital sovereignty" within state borders will continue to be reinforced. The examples of Turkey and other countries that are legally trying to introduce rules and restrictions for global social networks on their territory speak of the formation of a new sustainable trend in the Eurasian space - digital sovereignty.

The success of different states' attempts to ensure the "nationalization" and protection of the personal data of their population will directly depend on whether a particular country has the ability to create its own technological solutions and standards in the digital sphere. In fact, access to modern technological developments in the field of Big Data, artificial intelligence and 5G is becoming the most important guarantee of survival in the increasingly aggressive space of digital geopolitical competition. Players who are lagging behind in the digital race will eventually be deprived of the opportunity to fully ensure their own sovereignty, turning into "digital colonies" of the leaders of the global technological race.

5G TECHNOLOGY



Source: GSA 5G Market Snapshot

Steve Durbin
Chief Executive
Information Security Forum (ISF)
US Tel: +1 (347) 767 6772
UK Tel: +44 (0)20 3289 5884 | **UK Mobile:** +44 (0)7785 953800
steve.durbin@securityforum.org
securityforum.org

About the Information Security Forum

Founded in 1989, the ISF is an independent, not-for-profit association of leading organizations from around the world. The organization is dedicated to investigating, clarifying and resolving key issues in cyber, information security and risk management and developing best practice methodologies, processes and solutions that meet the business needs of its Members.

ISF Members benefit from harnessing and sharing in-depth knowledge and practical experience drawn from within their organizations and developed through an extensive research and work programme. The ISF provides a confidential forum and framework, which ensures that Members adopt leading-edge information security strategies and solutions.

By working together, ISF Members avoid the major expenditure required to reach the same goals on their own.

Consultancy services are available to support the implementation of ISF Products.

For more information on ISF Membership, please visit **www.securityforum.org**

+44 (0)20 3875 6868 | @SecurityForum | Information Security Forum