Tomorrow's Affairs
Analysis of today
Assessment of tomorrow

By: The Editorial Board

UK Law – worldwide privacy test

The Online Safety Bill is pending in the UK Parliament. It represents a continuation of the epic battle between governments and technology companies over the privacy of digital communications.

The scene is set, as it has been on many occasions before. The UK government's plan is for the law to oblige the owners of communication platforms to provide the Ofcom regulator an opportunity to monitor illegal content exchanged in private messages - from child sexual abuse material to terrorism.

Other governments had similar motives in previous cases, including the type of illegal content they wanted to monitor, usually to prevent terrorism or protect children from violent and inappropriate content.

Whatever the motives, governments wanted to push the boundaries and enter the space of free communications with no third-party oversight.
Michelle Donelan, secretary for Digital, Culture, Media, and Sport, previously explained her draft law by saying that the government "cannot let thousands of paedophiles get away with it".

A united voice against the law

Regulating and suppressing illegal content on online platforms is an important task for every government, but few have resisted stepping into the sphere of privacy, which could seriously threaten basic freedoms.

Never before have competing companies joined forces to resist restrictive legislation, as WhatsApp and Signal did in mid-April.

These popular communication platforms, along with five other encrypted chat apps, warned the UK government in an open letter that its law could be misused for disabling end-to-end encryption, that is, protected private communication.

“The bill poses an unprecedented threat to the privacy, safety and security of every UK citizen and the people with whom they communicate around the world, while emboldening hostile governments who may seek to draft copycat laws”, they stated in an open letter.

Their resistance raised several questions. The first, and certainly the most important, concerns the privacy of communications. Users of these platforms use them with full confidence to achieve uninterrupted and unsupervised communication with the other party.

They trust the service providers to secure sufficient protection (encryption) so that no third party, government, or private "observers" could access the communication.

After all, the right to unsupervised communication is an old asset of every democratic society. It used to refer to the inviolability of letters, later telephones, and today online messengers, for example.

The case of Blackberry

The second aspect is business, and concerns the survival of large and wealthy companies, which provide services to billions of people. The decline in trust in the privacy of communications through their platforms inevitably leads to collapse.

The experience of Canadian Blackberry is more than instructive in this regard, and none of the current communication service providers want something similar to happen to them.

Blackberry was an iconic system, a champion in protected end-to-end communication. Its users were business people, bankers, and people from government structures.
Its users included Hillary Clinton when she was US Secretary of State and Barack Obama, who barely agreed to hand over his Blackberry when he entered the White House as president.

Blackberry's star began to fall when, in 2010, it

started to make compromises with some governments, primarily in Asia, the UAE, or India, by allowing them to monitor previously protected communications.

Faced with threats of being cut off from traffic, the Company relented and allowed “back door" access, allowing governments to monitor communications (to curb terrorism and crime).

But Blackberry irretrievably lost its credibility, and the loss of users was inevitable. The company declared bankruptcy last year.

A dangerous precedent

The protest of the owners of communication platforms against the UK law that is in the process of being adopted is also a warning that the attempt to control encrypted communication is characteristic of autocratic systems, and by no means of an old and developed liberal democracy.
“We’ve recently been blocked in Iran, for example. But we’ve never seen a liberal democracy do that”, said Will Cathcart, Meta's head of WhatsApp, during a recent visit to the UK.

The responsibility of the UK is significant because if it passes such a controversial law, it will give legitimacy to any similar restrictive laws in any country of the world. After all, they will have a democratic precedent in the UK decision.

It is undeniable that thousands of terrorists, paedophiles, drug and weapon smugglers, and human traffickers all over the world communicate through chat platforms every day, as each of us does.

But they also communicate using phones, talk in restaurants, and write e-mails to each other. They use "ordinary" money and crypto-currencies, so it is impossible to introduce surveillance over every form of their communication to suppress their illegal activities.

Technology in itself is not a danger to society. It is useful. Abuse of technology is dangerous, but abuse cannot be stopped by a law whose effect is general and applies to everyone.

Illegal communications can be monitored, but based on a court decision, when there is a suspicion that it can harm society. The right to free and uncompromised communication is a fundamental civil and democratic right. It should not be monitored unless there is a specific reason.

Allowing governments and their regulators to "wander in the dark" by having access to every communication will not represent an effective fight against illegal and criminal activities, even if the "wandering" reveals a terrorist or a paedophile.

The privacy of billions of people on the right side of morality and law will conversely suffer irreparable damage.