Invasion of privacy

Telegram is not the ultimate privacy messenger you think it is.

Photo: 123rf.com

ANTI-GOVERNMENT protesters in Belarus, Hong Kong and Iran, Extinction Rebellion activists in Britain ... just about any organised group with something to fear from state officials uses Telegram to communicate.

The messenger app has long prided itself on refusing to hand over data to officials.

"That's why Telegram is banned by authoritarian governments such as Russia and Iran," said Telegram boss Pavel Durov, who himself is in exile from Russia after refusing to hand over user data to state officials.

Users, meanwhile, appreciate the message of privacy, the smooth interface and the public "channels" where like-minded people can discuss shared interests and causes.

And yet Telegram is a disaster in terms of user privacy, some security experts say.

Even before you send your message, the app sends every snippet and draft of text you type to Telegram servers in real time – whether or not you send it.

The server even has access to a complete copy of all chats, according to researchers at German industry specialist website Heise Security.

Your conversations should be stored exclusively on your own mobile device.

The problem: what Telegram does with your data, other than sending it to another mobile device, remains unknown.

Even WhatsApp offers more privacy assurances.

There are so-called "secret chats" as a Telegram function, which are secured to prevent third parties from reading them.

On its website, Telegram says if privacy security is an issue for you then you should use these secret chats with a self-destruct timer.

But these features are deactivated by default and so well hidden that most Telegram users aren't aware of them.

Secret chats are also more limited in functionality and won't work on more than one device you own.

Here, too, other messengers are better equipped – Signal, for example, or WhatsApp, which uses the encryption technology of Signal. There are no central chat databases for these two messengers.

The messages are encrypted so that only the real recipient can open and read them – in other words, end-to-end encryption.

The chats are also stored only on the owner's mobile device – never on remote servers that could theoretically be accessed by a court order.

But beyond that, we don't know much about the mechanics of the Facebook-owned app's inner workings, and it's entirely possible that backdoors have been built into WhatsApp's closed-source software.

Moreover, WhatsApp is gradually being integrated further into the Facebook group, which earns billions by processing its users' data to deliver targeted ads.

For a secure messenger alternative with good encryption, the experts recommend Signal, which is without exception open-source software.

This means that anyone with the know-how can check what is happening behind the scenes at any time.

In addition, the Signal infrastructure is operated by a non-profit foundation that is committed to data protection and is financed entirely by donations.

There is therefore no financial interest in the users' data. Telegram, on the other hand, is an opaque company construct, the motives for which are virtually unknown. – dpa