Published on substack
19 Dec 2025
Contact: alex.cyber@protonmail.com

www.AlexNotes.net

Türkiye: Use of Bylock evidence is a violation of human rights (European Court of Human Rights)

What this is about and why it remains relevant

Alexander Seger, 19 December 2025

The European Court of Human Rights (ECtHR) on 16 December 2025 confirmed that the approach of Turkish courts that anyone could be convicted for membership in an armed terrorist organization on the basis of the mere use of the Bylock messaging application was a breach of the rights against arbitrary prosecution, conviction and punishment and/or fair trial rights.

The decision was made following applications by 2420 Turkish nationals. This reiterates similar decisions of the ECtHR in September 2023 and July 2025.

What this is about

The Government of Türkiye attributed the attempted coup against president Erdogan of 15 July 2016 to the so-called "Gülen Movement" which is termed by the Turkish authorities the armed terrorist organization "Fetullahist Terror Organisation / Parallel State Structure" (Fetullahçı Terör Örgütü / Paralel Devlet Yapılanması) or "FETÖ/PDY".

Following the failed coup, hundreds of thousand of people were subjected to criminal proceedings (and over 125,000 convicted) for their alleged link to the Gülen Movement. More than 3,200 judges and prosecutors have been dismissed or arrested.

One of the criteria for determining membership in "FETÖ/PDY" was the installation or use of an encrypted messaging application called "Bylock". Over 100,000 people have been identified, investigated, arrested, detained or convicted because of the fact that they had installed or used Bylock or because their IP address had appeared in Bylock communications. The initial rational for these criminal proceedings seemed to have been provided by a technical report prepared by the Turkish National Intelligence Organization (MIT) that concluded that Bylock was developed by "FETÖ/PDY" and that it was "made available exclusively for members of the FETÖ/PDY armed terrorist organization". This conclusion has been - and keeps being - repeated over and over again by the government, the judiciary and pro-government media ever since.

In short, anyone having installed or used Bylock was and is considered a member of "FETÖ/PDY", membership in which incurs a penalty of 5 to 10 years of imprisonment.

In January 2017, the Istanbul Chief Public Prosecutor's Office prepared first indictments based on Bylock; thousands more followed. In early March 2017, it was reported that the MIT had sent a list of 122,000 ByLock users to the Ankara public prosecutor's office for further action.

In the course of 2017, the Constitutional Court of Turkey, and similarly the Supreme Court of Cassation, repeated the same argument, namely that Bylock was made available for use exclusively by members of the "FETÖ/PDY" armed terrorist organization for secure communication, and was thus evidence of membership in that organization.

Some judges that had dismissed the mere use of Bylock (without analysis of the content of a communication) as evidence were subsequently removed from their positions, thus raising further concerns regarding the independence of the judiciary in Turkey and their submission to political power.

ByLock was operational as an encrypted application from March 2014 until February or March 2016, that is, for a period of about two years. During much of that period it was available at Google Play and Apple Store from where it was downloaded some 600,000 times.

As a client-server application, ByLock required a server to function. Between 14 August 2014 and 2 April 2016, the ByLock server was hosted in Lithuania by the company Baltic Servers (now Cherry Servers), but reportedly went off-line in February or March 2016. This means that some four to five months before the failed coup of 15 July 2016, ByLock was not functional anymore. The MIT had obtained data (including on subscribers) from that server in Lithuania but information on how that occurred is conflicting and apparently not of particular interest to the Turkish courts. (According to a Supreme Court judge: "If someone finds a hard disk on the street and hands it to the police, of course the data can be used as evidence").

How this got to me

In the beginning of 2017, an insider from a Turkish criminal justice authority made me aware of the evolving Bylock drama in Turkey. (I was at the time heading the Council of Europe's Cybercrime Division and had close cooperation also with Turkey).

And so I started diving deep into it and carried out detailed research on questions such as whether Bylock use was indeed limited to members of the Gülen Movement, whether there was a link between the use of Bylock and the failed coup of July 2016, how the data on Bylock users has been obtained by the MIT, why information obtained by the MIT was admissible as evidence in criminal proceedings, etc.

In December 2017, I raised some of these questions with Turkish prosecutors and judges of the Supreme Court of Cassation. Their answers were confusing and contradictory. Their interpretation of some provisions of the Budapest Convention on Cybercrime was wrong. They didn't understand technology. They seemed to disregard the rather strong safeguards in the Constitution and criminal law of Turkey regarding the obtaining and admissibility of evidence. Considering the mere installation or use of Bylock as sufficient evidence of membership in an armed terrorist organization appeared to conflict even with criteria that the Supreme Court itself had established under prior case law.

At the end of December 2017, about two weeks after this exchange, the Turkish authorities began freeing hundreds of Bylock suspects, and the chief prosecutor of Ankara stated that they would review the cases of another 11,500 suspects. But they maintained that Bylock was strong evidence of membership in the Gülen movement.

One year later, in December 2018, I was invited to speak at an international workshop on cybercrime organized by the Turkish police near Ankara. Several hundred law enforcement officers, mostly from Turkey, participated.

After introductory remarks about positive cooperation with Turkey, I started to raise questions regarding Bylock and to refer to opinions of the Working Group on Arbitrary Detention of the UN Human Rights Council. That working group had two months earlier noted a "failure to show how the mere use of a regular communication application as ByLock constituted an illegal criminal activity" and that the "deprivation of liberty is arbitrary" (opinions 42/2018 and 44/2018 of October 2018).

In my intervention I underlined that for cooperation with Turkey in cybercrime matters reassurance was needed that laws and procedures are applied in practice and that rule of law requirements are respected.

The reaction by the audience was rather frosty, and I was subsequently photoshopped out of pictures taken during the event – but at least I made it home for Xmas.

All of this is to explain why I am pleased with the decision of the European Court of Human Rights of 16 December 2025 regarding "Further violations of the Convention in follow-up cases concerning convictions for terrorism offences based on use of Bylock messaging application".

And yes, even if it takes time: international courts are crucial for justice and accountability.

BUT!

The Turkish authorities keep arresting people that are suspected to be members of the Gülen movement based on Bylock. On 17 December 2025 – one day after the latest decision by the ECtHR – the pro-government news-paper "Daily Sabah" reported that "Security forces captured 160 FETÖ suspects in the past two weeks … Among targeted suspects were those communicating over Bylock …. Bylock is an encrypted messaging app developed and exclusively used by FETÖ members who also prefer public payphones to communicate with each other to avoid surveillance."

Obviously, the government of Turkey keeps ignoring the decisions of the European Court of Human Rights.

Authorities of other countries will need to consider carefully whether to cooperate with Turkey in cases and requests involving electronic evidence.

---

www.alexnotes.net