14-06-2022

Subject: Letter addressing the draft law on the collection and retention of identification data and metadata in the electronic communications sector and the provision of such data to authorities

Dear Members of the Parliament,

You are currently discussing the draft law on the collection and retention of identification data and metadata in the electronic communications sector and the provision of such data to authorities.

European Digital Rights (EDRi) is an association representing 47 human rights organisations from across Europe that defend rights and freedoms in the digital environment. Our network has been working on the issue of data retention for almost twenty years. Our members have engaged with policymakers on the risks for fundamental rights that such measure entails, provided technical expertise where possible and brought legislation to courts in Ireland, Austria, Germany, Czech Republic, the UK, France, etc. when these contravened national and European fundamental principles. Liga voor mensenrechten, which is working to broaden support for human rights in Belgium, has contributed to these efforts.

We welcome the attempt by the Belgian lawmakers to set up a legal framework in conformity with the Court of Justice of the European Union's (CJEU) case law for the retention of traffic and location data. Data retention regimes that are illegal under EU law must be abandoned and replaced as soon as possible with solutions that pass the strict necessity and proportionality test established by courts.

It is therefore essential that the new draft law that you are currently discussing does not introduce measures that would replicate the effects of the previous law on fundamental rights and that would be contrary to the Belgian Constitutional Court's and the CJEU's rulings.

Unfortunately, from our reading, this draft law, as it is and if adopted without adequate adjustments, would be a danger for people's rights, such as the right to privacy and data protection, freedom of expression and information, press freedoms and professional secrecy guarantees, and would potentially set a dangerous precedent for other Member States.

We identified the following several serious shortcomings that Parliament should urgently fix in order to avoid its future invalidation in courts:[1]

- **The strict necessity of Belgium's data retention law must be proven and not assumed:** Around the time of the invalidation of the previous data retention law by the Belgian Constitutional Court, police representatives warned that without data retention, the police would become "deaf and blind"[2] and argued that it was an indispensable measure.[3] However, mere political statements

1 For further details, we recommend to read l'avis de la Ligue des Droits Humains sur le projet de loi du 17 mars 2022 relatif à la collecte et à la conservation des données d'identification et des métadonnées dans le secteur des communications électroniques et à la fourniture de ces données aux autorités, 05.2022, https://www.liguedh.be/wp-content/uploads/2022/05/Avis-LDH-DATA-RETENTION-2022-final.pdf

2 *The Brussels Times*, Phone data investigations: Belgian law could be hanging by a thread, 31.03.2021, https://www.brusselstimes.com/162697/phone-data-investigations-belgian-law-could-be-hanging-by-a-thread-piloce-constitutional-court-service-providers-record-european-court-justice-crime-privacy

3 *RTBF*, Lutte contre le terrorisme : la conservation des métadonnées doit être exceptionnelle, selon le Comité T, 18.03.2022, https://www.rtbf.be/article/lutte-contre-le-terrorisme-la-conservation-des-metadonnees-doit-etre-exceptionnelle-selon-le-comite-t-10958051

pointing to the presumed value of data retention do not sufficiently substantiate the need for bulk retention of telecommunications data for the objective of investigating crimes. The mere usefulness of an instrument for law enforcement authorities does not satisfy the legality test, including necessity and proportionality. Instead, a fact-based assessment of the effectiveness of the measure is required, as well as the examination of less intrusive options that could achieve the same goal.

- **Targeted data retention must not lead to de facto mass data retention:** The CJEU case law allows the retention of metadata for a limited period of time only, in a targeted manner determined by a geographical criterion. The main conclusion is that the obligation to retain electronic communications data should be the exception, not the rule. The draft law chooses certain geographical areas according to rates of serious crime and to their nature to be subject to high risks of serious crimes, such as airports, railway stations, etc., where people present there would be placed under systematic data retention. The text specifies that "the government considers that it is not impossible for the entire national territory to be covered by data retention (...) If this hypothesis is met, it will then be a case of retention that is targeted in its approach but generalised in its consequences."[4] This would run counter to the very definition of "targeted": the crime threshold must therefore be adapted. Lastly, the new legislation would cover over-the-top (OTT) service providers[5] (such as WhatsApp, Skype, Signal or Facebook Messenger). These services cannot implement a geographical targeting of their users and will likely retain data on the entire Belgian territory. In addition, they are mostly established outside Belgium, and imposing these requirements in Belgian national law could conflict with the country of origin principle in EU law.

- **Targeted data retention should be based on objective criteria and verified data**: The data used to form the crime rates per geographical area would come from the National General Bank (BNG) which is known to contain numerous errors, inaccuracies and mischaracterisations. The use of the BNG as a statistical reference can therefore not be used to justify the infringement of the rights of such a large number of people.

- **The definition of serious crimes must be restricted**: The concept of serious offences as defined in Article 90ter of the Code of Criminal Procedure and used in the draft law to calculate the crime rate is too broad. It includes common law offences such as computer forgery, computer fraud, theft with violence, possession of narcotics and brings together offences that may lead to different penalty thresholds so that their serious nature does not seem to be objectified. Furthermore, the draft law requires operators to systematically store the data contained in the call detail record (CDR), the location data of suspects of a fraud or misuse of an electronic communications network, and the traffic data necessary to detect such fraud or misuse. However, fraud does not constitute a serious crime and thus, this retention obligation would be against EU law. Moreover, mobile operators increasingly offer flat-rate billing plans to their subscribers, making the retention of CDRs totally unnecessary for commercial reasons.

- **Only source IP addresses can be retained in bulk for fighting serious crimes**: The CJEU states that only the general and indiscriminate retention of IP addresses at the source of an electronic communication should be granted as an exception to the general prohibition of mass data retention. The proposed text allows the mass retention of categories of data beyond the strictly

4 Page 12 of the draft law, https://www.lachambre.be/FLWB/PDF/55/2572/55K2572001.pdf

5 OTTs are media services offered directly to viewers via the Internet. OTT bypasses cable, broadcast, and satellite television platforms; the types of companies that traditionally act as controllers or distributors of such content. It has also been used to describe no-carrier cellphones, with which all communications are charged as data, and that replace other call methods.

defined exception of the Court by including the identifier created for each call, the start date of the subscription or registration to the service, data relating to the type of payment or the identification number of the end-user terminal (International Mobile Equipment Identity, IMEI, Media Access Control, MAC or Permanent Equipment Identifier, PEI). The list should be restricted to what the CJEU prescribes and a limit to the retention period of IP addresses should be set by the legislator in line with the CJEU's requirements. We also suggest caution with regards to the retention of IP data as the new IPv6 standard allows to draw much more detailed conclusions about a person's life than previous connection data.[6] In the latest court case, the CJEU Advocate General confirmed that the problems arising from the use of the IPv6 protocol must be addressed in a future ruling.[7]

- **Belgium's data retention law must not undermine encryption:** The draft law confirms that it "prohibits an encryption system which makes it impossible for operators to retain identification, traffic or location data."[8] This goes further than the previous data retention obligation, under which a provider was only obliged to retain data generated or processed by them. Data that the provider did not collect could not be retained. The new legislation would force providers to record that data on behalf of the government, even if the provider doesn't see a need for itself. The consequences are potentially far-reaching, including world-wide, since the requirements would force these service providers to change their whole system, thus potentially putting users in authoritarian states at risk. It also means that chat services such as Signal will become illegal in Belgium. Signal is a secure encrypted communication system, on which many people (including journalists and politicians) rely for the safety and confidentiality of their communications. It does not collect more data than necessary to provide its services. The draft law would therefore put in jeopardy the availability of Signal in Belgium and thus, its use by Belgian citizens.[9]

We thank you for your consideration and remain at your disposal should you have any question.

Sincerely,

Chloé Berthélémy
Policy Advisor
chloe.berthelemy@edri.org

6 IPv6 allows for a unique IP address to be assigned to almost every device in our lives, notably connected devices such as watches, doors, toys and cars.
7 CJEU, Advocate General Opinion, Joined Cases C-793/19 and C-794/19, para. 83
8 Page 19 of the draft law, https://www.lachambre.be/FLWB/PDF/55/2572/55K2572001.pdf
9 Recent plans in the Netherlands to oblige chat apps, such as WhatsApp, to create back doors in their system to gain access to data were dropped after the company announced it would cease offering its services in the country. See Marc Hijink and Rik Wassens, 'WhatsApp dreigde uit Nederland te vertrekken om aftapplicht', *nrc*, 03.06.22, https://www.nrc.nl/nieuws/2022/06/03/whatsapp-dreigde-te-vertrekken-om-aftapplicht-a4132175