ICLE International Center for Law & Economics

Privacy, Crypto, and EU Financial Surveillance
July 11, 2022
Mikołaj Barczentewicz

European Union lawmakers appear close to finalizing a number of legislative proposals that aim to reform the EU's financial-regulation framework in response to the rise of cryptocurrencies. Prominent within the package are new anti-money laundering and "countering the financing of terrorism" rules (AML/CFT), including an extension of the so-called "travel rule." The travel rule, which currently applies to wire transfers managed by global banks, would be extended to require crypto-asset service providers to similarly collect and make available details about the originators and beneficiaries of crypto-asset transfers.

This legislative process proceeded with unusual haste in recent months, which partially explains why legal objections to the proposals have not been adequately addressed. The resulting legislation is fundamentally flawed to such an extent that some of its key features are clearly invalid under EU primary (treaty) law and liable to be struck down by the Court of Justice of the European Union (CJEU).

In this post, I will offer a brief overview of some of the concerns, which I also discuss in this recent Twitter thread. I focus primarily on the travel rule, which—in the light of EU primary law—constitutes a broad and indiscriminate surveillance regime for personal data. This characterization also applies to most of AML/CFT.

The CJEU, the EU's highest court, established a number of conditions that such legally mandated invasions of privacy must satisfy in order to be valid under EU primary law (the EU Charter of Fundamental Rights). The legal consequences of invalidity are illustrated well by the *Digital Rights Ireland* judgment, in which the CJEU struck down an entire piece of EU legislation (the Data Retention Directive). Alternatively, the CJEU could decide to interpret EU law *as if* it complied with primary law, even if that is contrary to the text.

The Travel Rule in the Transfer of Funds Regulation

The EU travel rule is currently contained in the 2015 Wire Transfer Regulation (WTR). But at the end of June, EU legislators reached a likely final deal on its replacement, the Transfer of Funds Regulation (TFR; see the original proposal from July 2021). I focus here on the TFR, but much of the argument also applies to the older WTR now in force.

The TFR imposes obligations on payment-system providers and providers of crypto-asset transfers (refer to here, collectively, as "service providers") to collect, retain, transfer to

other service providers, and—in some cases—report to state authorities:

> …information on payers and payees, accompanying transfers of funds, in any currency, and the information on originators and beneficiaries, accompanying transfers of crypto-assets, for the purposes of preventing, detecting and investigating money laundering and terrorist financing, where at least one of the payment or crypto-asset service providers involved in the transfer of funds or crypto-assets is established in the Union. (Article 1 TFR)

The TFR's scope extends to money transfers between bank accounts or other payment accounts, as well as transfers of crypto assets other than peer-to-peer transfers without the involvement of a service provider (Article 2 TFR). Hence, the scope of the TFR includes, but is not limited to, all those who send or receive bank transfers. This constitutes the vast majority of adult EU residents.

The information that service providers are obligated to collect and retain (under Articles 4, 10, 14, and 21 TFR) include data that allow for the identification of both sides of a transfer of funds (the parties' names, as well as the address, country, official personal document number, customer identification number, or the sender's date and place of birth) and for linking their identity with the (payment or crypto-asset) account number or crypto-asset wallet address. The TFR also obligates service providers to collect and retain additional data to verify the accuracy of the identifying information "on the basis of documents, data or information obtained from a reliable and independent source" (Articles 4(4), 7(3), 14(5), 16(2) TFR).

The scope of the obligation to collect and retain verification data is vague and is likely to lead service providers to require their customers to provide copies of passports, national ID documents, bank or payment-account statements, and utility bills, as is the case under the WTR and the 5th AML Directive. Such data is overwhelmingly likely to go beyond information on the civil identity of customers and will often, if not almost always, allow inferring even sensitive personal data about the customer.

The data-collection and retention obligations in the TFR are general and indiscriminate. No distinction is made in TFR's data-collection and retention provisions based on likelihood of a connection with criminal activity, except for verification data in the case of transfers of funds (an exception not applicable to crypto assets). Even, the distinction in the case of verification data for transfers of funds ("has reasonable grounds for suspecting money laundering or terrorist financing") arguably lacks the precision required under CJEU case law.

Analogies with the CJEU's Passenger Name Records Decision

In late June, following its established approach in similar cases, the CJEU gave its judgment in the *Ligue des droits humains* case, which challenged the EU and Belgian regimes on

passenger name records (PNR). The CJEU decided there that the applicable EU law, the PNR Directive, is valid under EU primary law. But it reached that result by interpreting some of the directive's provisions in ways contrary to their express language and by deciding that some national legal rules implementing the directive are invalid. Some features of the PNR regime that were challenged by the court are strikingly similar to the TFR regime.

First, just like the TFR, the PNR rules imposed a five-year data-retention period for the data of all passengers, even where there is no "objective evidence capable of establishing a risk that relates to terrorist offences or serious crime having an objective link, even if only an indirect one, with those passengers' air travel." The court decided that this was a disproportionate restriction of the rights to privacy and to the protection of personal data under Articles 5-7 of the EU Charter of Fundamental Rights. Instead of invalidating the relevant article of the PNR Directive, the CJEU reinterpreted it as if it only allowed for five-year retention in cases where there is evidence of a relevant connection to criminality.

Applying analogous reasoning to the TFR, which imposes an indiscriminate five-year data retention period in its Article 21, the conclusion must be that this TFR provision is invalid under Articles 7-8 of the charter. Article 21 TFR may, at minimum, need to be recast to apply only to that transaction data where there is "objective evidence capable of establishing a risk" that it is connected to serious crime. The court also considered the issue of government access to data that has already been collected. Under the CJEU's established interpretation of the EU Charter, "it is essential that access to retained data by the competent authorities be subject to a prior review carried out either by a court or by an independent administrative body." In the PNR regime, at least some countries (such as Belgium) assigned this role to their "passenger information units" (PIUs). The court noted that a PIU is "an authority competent for the prevention, detection, investigation and prosecution of terrorist offences and of serious crime, and that its staff members may be agents seconded from the competent authorities" (e.g. from police or intelligence authorities). But according to the court:

> That requirement of independence means that that authority must be a third party n relation to the authority which requests access to the data, in order that the former is able to carry out the review, free from any external influence. In particular, in the criminal field, the requirement of independence entails that the said authority, first, should not be involved in the conduct of the criminal investigation in question and, secondly, must have a neutral stance vis-a-vis the parties to the criminal proceedings …

The CJEU decided that PIUs do not satisfy this requirement of independence and, as such, cannot decide on government access to the retained data.

The TFR (especially its Article 19 on provision of information) does not provide for prior

independent review of access to retained data. To the extent that such a review is conducted by Financial Intelligence Units (FIUs) under the AML Directive, concerns arise very similar to the treatment of PIUs under the PNR regime. While Article 32 of the AML Directive requires FIUs to be independent, that doesn't necessarily mean that they are independent in the ways required of the authority that will decide access to retained data under Articles 7-8 of the EU Charter. For example, the AML Directive does not preclude the possibility of seconding public prosecutors, police, or intelligence officers to FIUs.

It is worth noting that none of the conclusions reached by the CJEU in the PNR case are novel; they are well-grounded in established precedent.

A General Proportionality Argument

Setting aside specific analogies with previous cases, the TFR clearly has not been accompanied by a more general and fundamental reflection on the proportionality of its basic scheme in the light of the EU Charter. A pressing question is whether the TFR's far-reaching restrictions of the rights established in Articles 7-8 of the EU Charter (and perhaps other rights, like freedom of expression in Article 11) are strictly necessary and proportionate.

Arguably, the AML/CFT regime—including the travel rule—are significantly more costly and more rights-restricting than potential alternatives. The basic problem is that there is no reliable data on the relative effectiveness of measures like the travel rule. Defenders of the current AML/CFT regime focus on evidence that it contributes to preventing or prosecuting *some* crime. But this is not the relevant question when it comes to proportionality. The relevant question is whether those measures are as effective or more effective than alternative, less costly, and more privacy-preserving alternatives.
One conservative estimate holds that AML compliance costs in Europe were "120 times the amount successfully recovered from criminals' and exceeded the estimated total of criminal funds (including funds not seized or identified)."

The fact that the current AML/CFT regime is a de facto global standard cannot serve as a sufficient justification either, given that EU fundamental law is perfectly comfortable in rejecting non-European law-enforcement practices (see the CJEU's decision in *Schrems*). The travel rule has been unquestioningly imported to EU law from U.S. law (via FATF), where the standards of constitutional protection of privacy are much different than under the EU Charter. This fact would likely be noticed by the Court of Justice in any putative challenge to the TFR or other elements of the AML/CFT regime.

Here, I only flag the possibility of a general proportionality challenge. Much more work needs to be done to flesh it out.

Conclusion

Due to the political and resource constraints of the EU legislative process, it is possible that

the legislative proposals in the financial-regulation package did not receive sufficient legal scrutiny from the perspective of their compatibility with the EU Charter of Fundamental Rights. This hypothesis would explain the presence of seemingly clear violations, such as the indiscriminate five-year data-retention period. Given that none of the proposals has, as yet, been voted into law, making the legislators aware of the problem may help to address at least some of the issues.

Legal arguments about the AML/CFT regime's incompatibility with the EU Charter should be accompanied with concrete alternative proposals to achieve the goals of preventing and combating serious crime that, according to the best evidence, the current AML/CFT regime does ineffectively. We need more regulatory imagination. For example, one part of the solution may be to properly staff and equip government agencies tasked with prosecuting financial crime.

But it's also possible that the proposals, including the TFR, will be adopted broadly without amendment. In that case, the main recourse available to EU citizens (or to any EU government) will be to challenge the legality of the measures before the Court of Justice.

View Article