

Diabolical Persistence

Oreste Pollicino

2020-07-25T11:15:47

As Genna Churches and Monika Zalnieriute wrote [here](#) on 16 July, the day on which the *Schrems II* decision was published, reading the judgment gives more than a simple feeling déjà vu; it rather looks like a full-blown Groundhog Day: One has the impression of being trapped in a time loop that forces us to relive the day – 6 October 2015 – on which the Court of Justice of the European Union (CJEU) adopted *Schrems I* and invalidated the European Commission’s [Safe Harbour Decision](#) (*Safe Harbour*) adopted on 26 July 2000.

Moving from cinema to the world of the classics, there is a famous Latin maxim according to which “*errare humanum est perseverare autem diabolicum*”, meaning “*whilst is it human to err, it is diabolical to persist with the same mistake*”.

More than a week after the *Schrems II* judgment was adopted, following the hundreds of comments made on the subject, I shall modestly attempt to consider the judgment (and the underlying saga) from two particular viewpoints, drawing inspiration from the Latin maxim mentioned above.

First of all, I shall focus on the diabolical persistence of the European Commission and secondly on judicial manipulation as the original sin of the CJEU and its (not so hidden) ambitions and frustrations (of not being a Constitutional Court).

1. The diabolical perseverance of the European Commission (for slightly more than two decades)

It is 15 May 2000 in Brussels. One of the giants of European Privacy, Stefano Rodotà, head of the Italian Data Protection Authority and the Working Party on Article 29, essentially authored the opinion in which that [Working Party](#) clearly set out its concerns on the Commission’s draft adequacy decision. The main concerns focused in particular on the need for clarity as regards the scope of *Safe Harbour*, the narrowing of exceptions and exemptions as well as the need for appropriate guarantees in relation to individual redress.

A few months later, on July 6, the European Parliament Report (Elena Paciotti as rapporteur and a fundamental rights defender) on the Commission’s draft clearly emphasised that “*adequate protection does not mean per se that the third country should have the same rules as the Union but that, regardless of the type of legislative protection in force in the third country, the data subject must be effectively protected*”. It then concluded solemnly, asking the European Commission “*to append this resolution to its transmission letter to the United States authorities, thereby clearly emphasising Parliament’s concern about the absence of an individual right of judicial appeal and the failure of an agreement to oblige companies to pay compensation for unlawfully processed data*”.

As can be imagined, the strong concerns were not enough to lead the European Commission to change its position, and the draft was approved without further amendment. Moreover, 15 years later the CJEU restated this basic position in *Schrems I*, pointing out exactly the same concerns as raised in 2000 by the Working Party on Article 29 and by the European Parliament.

The adequacy decision was invalidated, the *Safe Harbour* umbrella was torn, and there were reasonable expectations that a new transatlantic agreement would take on board the original concerns raised vocally by the CJEU.

The expectations became even greater after the CJEU had developed the new activist approach within its case law on the judicial enforcement of digital privacy: not only in *Schrems I* but also, less than a year before, [in *Digital Rights Ireland*](#) and [Google Spain](#).

[As it has been written by Giovanni De Gregorio](#) at the end of the last century, the Union adopted a liberal approach. A strict regulation of the online environment would have damaged the growth of the internal market, exactly when new technologies were going to revolutionize the entire society and promised new opportunities for the internal market. The end of this first liberal season was the consequent new activist approach by the CJEU, aiming at stricter intervention. This was the result of the Nice Charter as a bill of rights and new challenges raised by private actors in the digital environment.

In any case, the mentioned expectations essentially amounted to nothing: *Privacy Shield*, the successor of *Safe Harbour* did not fulfil them.

For the second time, the final compromise was a winning one for US commercial ambitions and a losing one for those who persisted in asking European Union negotiators to take privacy and data protection rights seriously as European constitutional rights enshrined in the European Charter of Fundamental Rights (ECFR).

Among the many weak points, two are particularly evident. They show that *Privacy Shield* did not correct the practical and legal issues associated with the Court's invalidation of *Safe Harbour* as the previous regime. First, the national security concerns of United States authorities appear to have enjoyed absolute primacy over the protection of personal data of EU citizens under the European Commission's arrangement with the United States. Secondly, there does not appear to be any mechanism for ensuring effective redress for EU citizens against such intrusions on fundamental rights. Both of these were already key arguments for the CJEU in invalidating the decision in *Schrems I* ([paras. 86-90](#)).

Against this backdrop, it would probably have been a set bet that, alongside Articles 7 and 8, the ECFR provisions engaged by the CJEU would have been Article 52 (proportionality) and Article 47 (right to an effective remedy)).

The Court held in relation to the former provision that U.S. surveillance programs, which the Commission assessed in its *Privacy Shield* decision, are not limited to

that which is strictly necessary and proportional, as is required by EU law. With respect to Article 47 ECFR, the Court held (surprise surprise, following the mantra of the last 20 years) that, as far as U.S. surveillance is concerned, EU data subjects lack actionable judicial redress and, therefore, do not have any right to an effective remedy in the U.S.

Before moving on to the second perspective, one question still remains as regards the diabolical perseverance of the European Commission. Would it not have been possible for the European Parliament to do more in advance, before the first and second adequacy decisions had been formally adopted?

The answer is, quite simply, 'no'. This is because, despite the persuasive efforts of Emilio De Capitani (executive director of the Fundamental Rights European Experts Group), the change of the relevant legal basis (from Directive 95/46 to the General Data Protection Regulation (GDPR)) did not alter the nature of the adequacy decisions taken by the Commission.

These are still executive discretionary acts and not legislative acts, for which the Commission's power to adopt an adequacy decision would be subject to stricter limits than today. It is sufficient to say that the Parliament and Council may revoke the delegation or express objections to any delegated act. This may be an opportunity lost, but there is still a window in the next European Commission's GDPR Review. So it would be best to avoid at least this kind of diabolical perseverance.

2. Judicial Manipulation of the CJEU reloaded and the training as a European Constitutional Court

The judicial manipulation by the CJEU in *Schrems I* is still fresh in our minds: *“even though an adequate level of protection does not require third countries to adopt an identical standard, individuals may nevertheless enjoy a degree of protection that is ‘substantially equivalent’ to that offered by EU law”* (para 73). The equivalence of the degree of protection is required, according to the Court, *“by virtue of an interpretation of the Data Protection Directive in light of the Charter”*.

The Charter thus becomes the legal device for the Court to raise the level of protection required under EU law by manipulating the parameter of “adequacy”, which is transformed in the different requirement of “essential equivalence”. The difference between these two criteria must not be neglected. The former does not imply a direct comparison between the EU and US level of protection, whilst the latter is based on such a comparison.

The GDPR did not codify the mentioned judicial manipulation in an explicit way. It may be the case that the same GDPR, at recital 104, states that “The third country should offer guarantees ensuring an adequate level of protection essentially equivalent to that ensured within the Union, in particular where personal data are processed in one or several specific sectors”. However, Article 45 still clarifies that such cases only involve an evaluation as to the adequacy of the level of protection, and not a comparison.

The CJEU did not want to lose the opportunity to propose the recalled judicial manipulation once again based on the shift from adequacy to essential equivalence.

The shift (and manipulation) was easier in this case than the first time (*Schrems I*) because of recital 104 (mentioned above). It should therefore come as no surprise when the Court asserts that:

“The first sentence of Article 45(1) of the GDPR provides that a transfer of personal data to a third country may be authorised by a Commission decision to the effect that that third country, a territory or one or more specified sectors within that third country, ensures an adequate level of protection. In that regard, although not requiring a third country to ensure a level of protection identical to that guaranteed in the EU legal order, the term ‘adequate level of protection’ must, as confirmed by recital 104 of that regulation, be understood as requiring the third country in fact to ensure, by reason of its domestic law or its international commitments, a level of protection of fundamental rights and freedoms that is essentially equivalent to that guaranteed within the European Union by virtue of the regulation, read in the light of the Charter”.

As we know from *Google Spain* and especially from *Digital Rights Ireland*, the Charter, as the European Bill of Rights, has thus far been the constitutional trump card played by the CJEU when engaging in judicial activism in order to enforce digital privacy rights. In doing so, it furthers its ambition of becoming (and reduces its frustration at not formally being) a proper constitutional Court. Let us consider the *Schrems* case with reference to the related narrative of the equivalence of protection for fundamental rights in Europe. It may come as a surprise that this narrative is appealing for the CJEU, much more than the adequacy narrative. Only the former links up the judicial frame in *Schrems (I and II)* with the broader narrative of constitutional adjudication in European constitutional law, from *Solange* through to the *Kadi*, not forgetting *Bosphorus*.

Here too there is nothing new under the sun; it amounts as it were to another trial run for the CJEU in order to be fully ready to play a proper role as a pan-European Constitutional Court.

Final remarks

In conclusion, what needs to be properly investigated are the judgment’s implications for the new roles (and new responsibilities) of data controllers and, more generally, for digital platforms in the new legal scenario related to data transfer to third countries. However, one message coming from Luxembourg seems clear enough also from a first reading: the data exporter will face a quite complex and delicate evaluation, which implies further responsibility especially for platforms with the difficult dual status of hosting provider and data controller.

Spiderman might tell us that with great power comes great responsibility; and yet as every constitutional scholar knows full well, constitutionalism concerns the limits of power, and in this case the challenge is how to face new private

digital powers as the geometry of power is shifting from a vertical to a horizontal dimension. It is becoming clearer that the path will lead towards further increasing the responsibilities of intermediaries.

