Casarosa, Federica

Article

Transnational collective actions for cross-border data protection violations

Internet Policy Review

Provided in Cooperation with:
Alexander von Humboldt Institute for Internet and Society (HIIG), Berlin

Suggested Citation: Casarosa, Federica (2020) : Transnational collective actions for cross-border data protection violations, Internet Policy Review, ISSN 2197-6775, Alexander von Humboldt Institute for Internet and Society, Berlin, Vol. 9, Iss. 3, pp. 1-14, https://doi.org/10.14763/2020.3.1498

This Version is available at:
https://hdl.handle.net/10419/224938

INTERNET POLICY REVIEW
Journal on internet regulation

Volume 9 | Issue 3

Transnational collective actions for cross-border data protection violations

Federica Casarosa
Centre for Judicial Cooperation, European University Institute, Fiesole, Italy,
federica.casarosa@eui.eu

Published on 16 Sep 2020 | DOI: 10.14763/2020.3.1498

Abstract: With the Cambridge Analytica/Facebook scandal, online surveillance clearly showed its negative effects. However, few individuals were able to recover any damages from the data protection violation that occurred. The EU General Data Protection Regulation contains legal tools to coordinate the interests of data subjects together in the case of infringements that occur across member states of the European Union, not only at the national level (Article 80), but potentially at the transnational level, as implied by Article 81. However, only a reform addressing the rules applicable to the standing of associations and non-governmental organisations in transnational claims as well as those concerning jurisdiction and international lis pendens would allow EU citizens to take full advantage of this opportunity.

Keywords: Surveillance, Collective redress, Transnational collective action, Data protection, GDPR

Article information

Received: 26 Sep 2019 **Reviewed:** 19 Dec 2019 **Published:** 16 Sep 2020

Competing interests: The author has declared that no competing interests exist that have influenced the text.

URL:
http://policyreview.info/articles/analysis/transnational-collective-actions-cross-border-data-protection-violations

Citation: Casarosa, F. (2020). Transnational collective actions for cross-border data protection violations. *Internet Policy Review*, *9*(3). DOI: 10.14763/2020.3.1498

This paper is part of Geopolitics, jurisdiction and surveillance, a special issue of Internet Policy Review *guest-edited by Monique Mann and Angela Daly.*

INTRODUCTION

The Cambridge Analytica/Facebook (hereinafter CA/FB) scandal revealed the level of surveillance we may be subject to during the time we spend online. The fact that a Facebook app was programmed to gather personal data from more than 87 million users' profiles without their consent shows how crucial data gathering is for online platforms. The CA/FB case was shocking

for two main reasons: first, because the collection of data was concealed within a quiz app able to access not only information in the profiles but also about the 'friends' of the people that took the quiz; and second, and most importantly, because Facebook CEO Mark Zuckerberg did not decide to notify the competent authorities of the unlawful data processing immediately, even though he was aware that the data gathered were subsequently sold to Cambridge Analytica. Instead the Facebook CEO only asked the profiling company to destroy the information obtained unlawfully without checking for subsequent confirmation (Messina, 2019). As a result, Cambridge Analytica used the data to profile users and target potential voters with personalised political messages during the 2016 US election (Cadwalladr, 2018; Granville, 2018).

We live in a data-driven economy where personal data can (consciously or not) be used as counter-performance for digital services. This process started, according to Zuboff (2019), in 2002 when society moved towards a form of 'surveillance capitalism', which is based on the instrumentalisation of human behaviour for the purposes of modification and monetisation.

This is reflected in the business model adopted by online platforms, which use data as fuel: without data on users' activities no advertisement may be sold nor a new app developed. This is the reason why platform data gathering is increasing, both in terms of breath and depth. According to Manokha (2018), user data gathered by Google include several types of information such as: the user's location (via smartphone use); search history across devices; app and extensions used, including frequency of use and contacts; parent company (such as YouTube) history; bookmarks, emails and contacts when Google products are used. Moreover, when more devices are connected, each of them may provide additional data. The depth of data gathering flows from the ever-improving technical tools used by online platforms, exploiting algorithms and more recently artificial intelligence (AI) to process data and develop profiles and clusters of users.

However, this approach is not without limits and one of the most pervasive and detailed regulatory frameworks to safeguard users' data is data protection. One of the pillars of this, both in the European Union and in the US, is user consent, which should be based on the data subject being aware of – and (in theory) understanding – the processing of their data and the potential consequences. [1]

In the CA/FB case, data subjects were clearly not aware of the type and objectives of the processing, not having consented to a further use of the data gathered by the app. The social networking platform failed to perform the monitoring tasks allocated to the data processor in the case of a breach. From a legal perspective this was unlawful data processing which could be subject to judicial and administrative proceedings, which was exactly what happened in a few European countries, namely the UK, Italy and Germany.

In the UK, the Information Commissioner's Office (ICO) extended the investigation it was already conducting into data analytics for political purposes to encompass the CA/FB scandal, eventually announcing its intention to fine Facebook for lack of transparency and security issues relating to the harvesting of data in contravention of the Data Protection Act 1998. Then, in October 2018 it fined Facebook £500,000 for breaching the UK's data protection law. Discussing the numerous reasons for imposing the maximum fine, the ICO noted "the personal information of at least one million UK users was among the harvested data and consequently put at risk of further misuse". In Italy, in April 2018 both the Italian Data Protection Authority (DPA) and Antitrust Authority started an investigation into what exactly happened with the data, both in terms of individual privacy and alleged unfair commercial practices. Eventually the investigations resulted in one of the highest fines by the Italian DPA, on the basis of Facebook's

economic status and the number of its users both worldwide and in Italy (Italian Data Protection Authority, 2019).

In all these cases, the administrative procedure was initiated *ex officio* by DPAs as a reaction to data breaches that occurred in relation to domestic users in each country, whereas no individual user was able (or willing) to claim before national courts for the same data breaches. The data breaches were negligible for each individual, which is clearly a disincentive to starting a long and expensive judicial procedure that could result in a very limited award of damages. As a result, users were not able to recover any damages due to practical limitations affecting their right of access to justice.

While at the societal level the fines imposed by the national DPAs on the overall data protection system may trigger the adoption of better and stronger means for online platforms to protect personal data under the threat of higher fines and stricter scrutiny of their conduct, they do not provide specific redress for each citizen who has suffered from the violation. Moreover, in the case of cross-border data processing in the EU, the intervention of DPAs is subject to a coordination mechanism which requires the identification of a lead supervisory authority that will guide the investigation activities of the other DPAs involved, pursuant to Article 56 GDPR (Article 29 Data Protection Working Party, 2017). Given that the identification of the lead supervisory authority is based on the main establishment of the data processor, there may be a risk of forum shopping towards countries where the enforcement of (joint) decisions is less vigorous (a phenomenon also seen regarding encryption measures - see Mann et al., 2020). The need for an intervention enhancing cooperation among data protection authorities was also affirmed by the European Commissioner Věra Jourová (European Commission, 2020), however, so far no specific action has been taken in this direction.

The position of data subjects is still weaker *vis-à-vis* that of data processors, particularly in the case of big online companies, which may justify their activities on the ground that limiting access and use of data would have the effect of limiting the opportunities that large volumes of data may offer in terms of personalisation, cost reduction etc. In order to achieve an effective remedy when breaches occur, there is a need for alternative forms of enforcement such as collective redress which may empower data subjects *vis-à-vis* data processors - particularly in cases where a public outcry regarding data breaches does not result in such swift and immediate administrative proceedings before DPAs (Manokha, 2018; Messina, 2019). Collective remedies may thus provide for the effective protection of data subjects' interests through what has been claimed as a need for the active empowerment of individuals (Malgieri and Custers, 2017).

Within this framework, some steps were taken by the EU legislator in drafting the General Data Protection Regulation (GDPR), [2] which introduced the possibility for data subjects to also exercise their rights through associations and non-profit organisations. According to Article 80, a data subject "shall have the right to mandate a not-for-profit body, organisation or association […] to lodge the complaint on his or her behalf, to exercise the rights referred to in Articles 77, 78 and 79 on his or her behalf, and to exercise the right to receive compensation referred to in Article 82 on his or her behalf where provided for by Member State law".

Although there are several open issues regarding better solutions to implement this provision at the national level, it is interesting to note that an element that is crucial in the online environment is the possibility of coordinating actions across different EU member states when violations occur in several countries as a result of the conduct. This element is addressed in Article 81 GDPR, which provides a special rule on lis pendens in cases where the same data controller or processor is party to different proceedings in different EU member states, or the

proceedings concern the same subject. [3] Indeed, Article 81(2) GDPR provides that "where proceedings concerning the same subject matter as regards processing of the same controller or processor are pending in a court in another Member State, any competent court other than the court first seized may suspend its proceedings".

This provision paves the way for transnational collective actions, which in principle may achieve positive results for both parties:

- for multinational companies that have seats in different EU countries - they will not have to be subject to proceedings across the EU for the same conduct but with different procedural rules;
- for national associations and NGOs working on data protection issues, which will have the opportunity to strengthen their position *vis-à-vis* data processors as a result of a wider range and larger number of claimants. At the same time they will be able to collaborate and coordinate their actions across the EU, thus reducing the costs of multiple proceedings in different courts in EU member states.

This contribution will focus on the current framework provided for transnational collective actions. It will show the gaps emerging in legislation, the limits set by private international law rules on jurisdiction over such actions, and the consequences that these actions may have for the coordinating mechanisms between national courts and data protection authorities. In particular, Section 2 will provide an overview of the collective redress mechanism provided by the GDPR and in Section 3 the specific issues related to transnational collective claims will be addressed.

COLLECTIVE REMEDIES IN THE GDPR

Collective remedies or collective redress mechanisms include a large number of legal instruments aimed at resolving disputes by clustering multiple individuals within a single action or procedure. According to Hodges (2019), the collective enforcement mechanisms that can be identified are private collective litigation, the *partie civile* mechanism (a civil claim following on from a criminal prosecution), the involvement of public regulatory authorities (either through the power to order redress by starting a collective court claim or merely through the general enforcement authority) and Alternative Dispute Resolution (ADR), namely through the Consumer Ombudsman.

This contribution will only focus on the two possible options for the first mechanism, namely (a) the procedure granting a member of the affected group standing to bring an action on behalf of the group (a so-called class action or group action) and (b) the procedure granting a representative entity standing to bring an action on behalf of the group (a so-called representative action). In both cases, a group of claimants sharing the same interest starts the action, and a single representative or an association represents the entire group. Then, according to procedural rules, the representative (be it an individual or an association) is in charge of pursuing the action, while the other individual members do not play a role in the proceedings.

The objective of these types of actions can be simply compensatory, allocating the damages caused by the violation to each of the group members, or may be to achieve deterrent effects, in particular through injunctive relief preventing future violations (Hodges, 2019; Bosters, 2017; Trstenjak and Weingerl, 2014).

Although the EU legislator left the task of putting this provision into practice to the member states by introducing substantive and procedural rules applicable to collective redress (Casarosa,

2018; Pato, 2019), I note some important features emerging from the current legislative framework.

According to Article 80 GDPR, each member state should provide for three different types of action:

- an opt-in collective action in which the interested parties have the right to instruct an authorised body to file a complaint on their behalf, the right to lodge a complaint with a supervisory authority (Article 77 GDPR), the right to an effective judicial remedy against a supervisory authority (Article 78 GDPR) and the right to an effective judicial remedy against a controller or a processor (Article 79 GDPR);
- an opt-in collective action in which the interested parties have the right to instruct an authorised body to exercise the right to receive compensation, but only if the legislation of the member state so permits;
- an opt-out collective action where the authorised entities are authorised to act on behalf of the data subjects without having obtained a mandate from those persons in the case of infringement of the rights of a data subject under the Regulation, as long as the member state provides for such a possibility. Claims for compensation are, however, excluded from this mechanism.

In the opt-in procedures, it is clear that data subjects will have to take positive steps to join the proceedings, affirming their rights and the will to be subject to the effects of the decision. In these scenarios, however, the GDPR does not preclude the possibility for member states to identify different phases of the judicial or administrative proceedings in which the opt-in may take place. The opt-out procedure instead implies that the group of claimants is not identified individually. However, the decision of the court will bind all groups sharing the same interest. To be outside the group, data subjects have the possibility of opting out (Bosters, 2017).

Each member state is free to select whether all three actions will be available or only the first (and mandatory) one. This choice would also be based on the pre-existing national legislation applicable to collective redress, which in some member states already covers data protection. [4]

Regarding the application of procedural rules in the case of collective actions, the GDPR is silent, leaving the national legislator full discretion. As for the applicable forum, guidelines emerge in Article 79(2) GDPR, which expressly provides that (individual) actions before the courts should be brought in the member state where the controller or the processor is established. Alternatively, such actions may be brought before the courts of the member state where the data subject is habitually resident. However, in this case it is difficult to identify if habitual residence is applicable as more data subjects are involved in the claim who may be resident in different countries, although no criteria of preference is provided. Moreover, in the case of associations or NGOs the criteria of habitual residence cannot be applicable (Casarosa, 2018). As a result, it will be up to the national legislators to identify the procedural rules applicable to this type of case: for instance, in Italy, the solution adopted allocated jurisdiction to the tribunal of the place where the controller or the processor is established also in those cases where the claim is presented by an association (as provided by Article 10 of the amended Legislative decree 151/2011).

Other doubts emerge, in particular regarding the effect of a decision declaring a violation of the data protection rules which may or may not also include an award of damages to the data subjects. In the event that the member state provides for an opt-out collective action, where an association or an NGO is authorised to act on behalf of the data subjects without any individual mandate, which effects will the decision of the judicial authority have *vis-à-vis* the data subjects that did not take part in the action? According to Article 80 GDPR, member states are free to

include this procedure, but the article is silent on the third party effects of the decision. Would it be possible for a decision declaring a breach of data protection rules to be followed by so-called follow-on actions by individual data subjects to obtain any compensation for the damage suffered as a result of the violation? Similar doubts emerge in the case of opt-in collective claims. Where a mandate is provided by a limited number of data subjects, what would be the effect of a decision declaring that the conduct of the data controller does not infringe data protection rules? Can such a decision limit any subsequent claim pursued through individual proceedings? Or would it only be used in such proceedings by the defendant as proof of lack of wrongdoing?

Obviously, these elements may be decided at the national level following pre-existing procedural rules. However, given the EU's recent attention to collective remedies in the consumer protection sector (European Commission, 2018), the rules applicable should be carefully identified. It is interesting to note that in the context of EU intervention in relation to collective actions, a much more effective approach has been adopted in the Proposal for a Directive of the European Parliament and of the Council on representative actions for the protection of the collective interests of consumers, and repealing Directive 2009/22/EC, COM(2018) 184 final. Also in this case the legislator has taken on board the problems that arose as a result of cases of infringement that have occurred in the member states. First and foremost in the Dieselgate case (Garaci and Montinaro, 2019), where the collective protection of users came up against the difficulty of recognising the effects of the decisions of individual member states' competition authorities on collective actions relating to the same infringements. The Proposal for a Directive in fact addresses the cases where there is an interaction between administrative enforcement (for instance through DPA involvement) and judicial enforcement. Article 10 of the Proposal for a Directive states that final decisions (regardless of their objective and the deciding body) are considered evidence (freely assessable by the court) that establishes the existence or non-existence of an infringement, for the purposes of any other action for damages before national courts against the same controller or processor, on the same facts.

Given that there may well be cases where there is an overlap between the status of consumer and of data subject, the rules applicable to collective claims in the consumer and data protection frameworks should provide for an even level of judicial protection (Amaro et al., 2018; Casarosa, 2020). For example, a collective action based on a claim of unfair contractual clauses included in the so-called privacy policy attached as contractual content to the terms of service of several online platforms may be used for both injunctive and compensatory claims, but (according to the proposed Directive on collective claims for consumer protection) other consumers who are in the same contractual scenario are also allowed to use the decision as evidence for bringing equivalent claims for damages. The same cannot happen for collective actions for claims regarding the violation of data protection rules. Thus, a situation of unequal judicial protection could arise which is not justified by substantive differences (Casarosa, 2018).

The degree of complexity increases when looking at the possibility of transnational collective claims.

TRANSNATIONAL COLLECTIVE ACTIONS

Although collective claims are perceived as a tool to safeguard the interests of a plurality of claimants unable to pursue their interests through judicial proceedings, the existing legal framework applicable to collective actions at EU, and consequently at national level, seems to

rely on the assumption that only national collective redress is conceivable (Amaro et al., 2018, p. 94). This assumption did not hold when the *Schrems v Facebook* case arrived at the Court of Justice of the EU (CJEU) in 2018.

The C-498/16 *Schrems v Facebook* case was the first example of the possible use of collective actions at the transnational level in the field of data protection. The case involved Maximillian Schrems, who presented a claim for alleged violation of data protection laws in his own country (Austria). The claim was not only in his name but also in the name of seven other claimants resident in other EU member states and in non-EU countries. These other claimants provided a mandate to Mr Schrems to act on their behalf, following the Austrian law allowing for different claims to be presented by one applicant against the same defendant. [5] The national court, however, had several doubts regarding the qualification of Mr Schrems as a consumer as he was involved in several academic and commercial activities, first as a privacy activist and then as the founder of a non-profit organisation, NOYB – European Center for Digital Rights. The qualification of the status of Mr Schrems impacted also on whether the protective provisions in the Brussels I Regulation were applicable. According to Article 18 Brussels I Regulation "a consumer may bring proceedings against the other party to a contract either in the courts of the Member State in which that party is domiciled or, regardless of the domicile of the other party, in the courts of the place where the consumer is domiciled". The qualification as a consumer, then, would allow Mr Schrems to bring the claims ceded to him before the Vienna jurisdiction. The CJEU's decision addressed the analysis of the application of the Brussels I Regulation with some caution (Amaro et al., 2018) due to the fact that any extended interpretation of Article 18 of the Brussels I Regulation regulating the consumer forum would have the indirect effect of reducing legal certainty, as the representative of the consumer group may be allowed to select the forum from those available to the group (Blanc, 2017).

This case showed clearly that given the ubiquitous control occurring of personal data online, it is possible (if not common) that the same conduct occurring in different member states may result in a violation of the data protection framework against a large number of online users. In this case, there are two possible options: one is the emergence of several national collective actions against the same defendant, following in each case the rules and procedures applicable at the national level. This was the path selected, for instance, by consumer associations in Belgium, Spain, Portugal and Italy, which followed a collective strategy: each association presented a national collective claim against Facebook in relation to the Cambridge Analytics/Facebook scandal (Consumer International, 2018). In this case, however, the decisions of courts at the national level may differ, and such decisions may not be used as an authoritative precedent in foreign countries. The alternative available is the transnational collective claim: this claim may avoid the fragmentation of the proceedings and of the decisions, collecting all the claims within a single procedure.

Although in practice this case is far from unrealistic, the possibility of pursuing a transnational collective action faces several difficulties.

As mentioned above, Article 81 GDPR hints at cases where data processors may be sued in different countries for the same violation, alluding to the occurrence of a cross-border dimension of the violation. However, the Article does not specify if it only applies to individual claims or to collective claims. If a claim presented by an association represents data subjects in different EU countries, which are the rules applicable according to the current EU legal framework?

The first issue is legal standing: can associations and NGOs which qualify to represent data

subjects in national collective actions also be able to present transnational claims? The GDPR does not provide any indication, but neither does it exclude this possibility. A comparison with Injunction Directive 2009/22/EC [6] can help by acknowledging that this element is not without importance: Recital 12 of the Directive provides that mutual recognition should apply in the case of associations and NGOs which have been admitted as qualified claimants at the national level. The provision then prevents requirements identified for the qualification from being interpreted differently across countries, thus avoiding conflicting judgments on the admissibility or recognition of collective redress actions (Voet, 2017). Given that Article 80 GDPR already identifies the basic requirements for associations and NGOs, it would be reasonable to acknowledge that they should be applicable across the EU.

An additional element highlighted by ELI/Unidroit (2018) in a chapter dedicated to the model rules on collective redress is the fact that information regarding collective actions across Europe would also be fruitful in order to avoid parallel proceedings and enhance cooperation among European actors. According to Articles [X4bis] and [X29], national courts should provide a publicly accessible electronic register where all collective redress claims are registered in order for potential 'qualified claimants', lawyers, group members etc. to gain knowledge of existing actions. When such collective claims have a cross-border effect, the model rules provide that the registry entries "shall be made available on the European e-justice platform". However, it must be highlighted that the disclosure of the name of the defendant in such cases could have adverse effects on their position, in particular when liability is still to be decided, as clarified by Articles 35-36 of the European Commission Recommendation on common principles for injunctive and compensatory collective redress mechanisms. [7]

Another important set of questions relate to the private international laws (here after PILs) applicable in the case of transnational collective claims. As is clearly acknowledged by the Report on Collective Redress (2018) (and previously Voet, 2017; Money-Kyrle, 2016), the current legal framework for PILs is still unsatisfactory. The applicable EU Regulations, namely the Brussels I Regulation [8] and the Rome I [9] and Rome II [10] Regulations are all drafted taking as the point of reference a conflict between an individual claimant and an individual defendant.

Only Article 4 of the Brussels I Regulation provides the possibility of multiple claims being consolidated, and in this case the general rule regarding the choice of jurisdiction designates the defendant's domicile. Accordingly, any collective action for data protection infringement would be obliged to sue the data controller at its headquarters in any EU member state, for instance Ireland in the case of Facebook. This would create the possibility for data controllers to select safe havens in member states where collective redress mechanisms are not effectively regulated. Moreover, the special rule in Article 7 (2) Brussels I Regulation does not provide an effective solution as it affirms that, in the case of tort, delict or quasi-delict, the claimant may sue before the court of the place where the harmful event occurred. This permits cases of concurrent jurisdiction. Only if the defendant proves that the harmful event occurred in the place where the decisions regarding the data processing were taken, i.e. at the headquarters of the data processor, will there be no difference in the application of the general rule provided by Article 4 Brussels I.

In the case of concurrent jurisdiction, rules on lis pendens may apply, and as mentioned above Article 81 GDPR provides for a *lex specialis* vis-à-vis Articles 29-34 Brussels I Regulation. Article 81 GDPR provides that if the defendant (i.e. the data controller or processor) coincides in both proceedings or the claims address the same conduct, the court subsequently seized may suspend the action in order to await the outcome of the proceedings before the foreign

authority. Moreover, the Article recognises the possibility for courts to decline jurisdiction at the request of one of the parties if "the court first seized has jurisdiction over the proposed actions and its law allows proceedings to be joined" (Article 81(3)). If the provision also applies to collective actions, then parallel proceedings may be avoided if the national procedural rules allow consolidation of actions.

Instead, in the case where procedural rules do not allow for consolidation of proceedings, it is important to consider the effects the decisions of the foreign court may have on the suspended proceedings. What is the value of a foreign decision in a parallel proceeding? On the one hand, a decision in a collective claim is automatically recognised in the other member states according to Article 36 of the Brussels I Regulation without any specific procedure. On the other hand, the decision may be used in the suspended proceeding as proof of the existence or non-existence of the violation, which can be evaluated by the judge. However, no specific guideline is provided by the EU legislator as regards the role of the decision.

As emerging from the analysis here, it seems clear that transnational collective claims in the data protection area cannot be exploited *yet*. In particular, the provisions of Brussels I Regulation dedicated to jurisdiction and lis pendens are not apt for addressing multi-party conflicts. Thus, a further step is needed from the EU bodies, namely an effort to coordinate the specificities of the GDPR enforcement system with amended private international law rules in order to provide an effective transnational collective action that can enhance the opportunities for data subjects to enforce their rights.

CONCLUSION

The GDPR was seen as a step forward in solving many of the challenges posed by the development of new technologies, and in particular it was presented as a tool to improve data subjects' awareness and to empower them *vis-à-vis* data processors through consent mechanisms, avoiding hidden data processing. Reality has then clashed against this positive image, as the CA/FB scandal arose just before the entry into force of the GDPR. The case showed that forms of surveillance over online users are more and more subtle and able to manipulate the choices of users not only over goods and services but also political preferences, with significant implications for democratic processes. Given the data protection framework, if preventive measures do not achieve the result of protection, then data subjects should at least have access to remedial measures that can help them recover potential damages, and through collective action overcome the weaker position each individual user may have *vis-à-vis* data processors.

The GDPR framework has already made a step forward in this direction by requiring member states to adopt national provisions for collective actions. However, given the cross-border nature of violations of data protection rules occurring online, the objective should be even more ambitious: to address the possibility of presenting transnational collective actions where associations or NGOs may represent claimants from different EU countries. It is true that the current framework includes some common principles regarding the features that associations and NGOs should have in order to engage in collective actions before national courts, ensuring – in principle – equivalent criteria across the EU. However, the EU legislator could have explicitly mentioned in addition that the mutual recognition principle (applicable to other collective actions according to Directive 2009/22 on injunctions) is also applicable to any entity designated for such collective actions at the national level. Accordingly, lists of organisations

qualified according to national criteria could be communicated to the Commission and publication in such a list could be used as proof of legal capacity in other EU member states' national jurisdictions. [11]

Moreover, the system provided by the GDPR is based on the assumption that not only are qualified associations and NGOs aware of existing collective actions but also that data subjects are aware of breaches occurring at a cross-border level, are interested in joining such actions and provide their mandate to the relevant association or NGO. Unfortunately, such active engagement of data subjects is difficult to find in practice and the lack of centralised information mechanisms is an open issue in the development of transnational collective actions. The proposal by the ELI/UNIDROIT group regarding the creation of an electronic register of existing collective actions could be seen as a simple yet effective tool to improve the ability of qualified organisations to collaborate in the case of cross-border actions.

Finally, a revision of the EU legal framework regarding the private international law rules applicable to transnational collective claims and the effects that transnational decisions may have is required. If the process of modernisation of collective redress mechanisms – which started in 2013 with the Recommendation on common principles for injunctive and compensatory collective redress mechanisms – is not to end, increased attention should be dedicated by the EU legislator to ensuring EU citizens have effective access to transnational collective actions.

REFERENCES

Amaro, R., Azar-Baud, M. J., Corneloup, S., Fauvarque-Cosson, B., & Jault-Seseke, F. (2018). *Study on Collective Redress In the Member States of the European Union* [Study]. European Parliament. http://www.europarl.europa.eu/RegData/etudes/STUD/2018/608829/IPOL_STU(2018)608829_EN.pdf

Article 29 Data Protection Working Party. (2017). *Guidelines for identifying a controller or processor's lead supervisory authority. 16/EN WP 244 rev.01*. http://ec.europa.eu/newsroom/document.cfm?doc_id=44102

Biard, A. (2016). *Class Action Developments in France* [Country report]. Global Class Actions Exchange. http://globalclassactions.stanford.edu/content/class-action-developments-france

Blanc, N. (2017). Schrems v Facebook: Jurisdiction Over Consumer Contracts Before the CJEU. *European Data Protection Law Review*, *3*(3), 413 – 417. https://doi.org/10.21552/edpl/2017/3/20

Bosters, T. (2017). *Collective Redress and Private International Law in the EU*. Asser Press.

Cadwalladr, C. (2018, March 18). I made Steve Bannon's psychological warfare tool': Meet the data war whistleblower. *The Guardian*. https://www.theguardian.com/news/2018/mar/17/data-war-whistleblower-christopher-wylie-faceook-nix-bannon-trump

Casarosa, F. (forthcoming). Azioni collettive fra tutela dei dati personali e tutela dei consumatori: Nuovi strumenti alla prova dei fatti. In P. Iamiceli (Ed.), *Diritti Fondamentali ed effettività della tutela*. Uni Service.

Casarosa, F. (2018). La tutela aggregata dei dati personali nel Regolamento UE 2016/679—Una base per l'introduzione di rimedi collettivi? In M. A. & D. Poletti (Eds.), *Regolare la tecnologia: Il Reg. UE 2016/679 e la protezione dei dati personali. Un dialogo fra Italia e Spagna*. Pisa University Press.

Consumers International. (2018). Not your Puppets: An update on the Euroconsumers class action against Facebook [Blog post]. *Consumers International*. https://www.consumersinternational.org/news-resources/blog/posts/not-your-puppets-euroconsumers-interview/

D. Messina. (2018). Il Regolamento (EU) 2016/679 in materia di protezione dei dati personali alla luce della vicenda 'Cambridge Analytica'. *Federalismi.it*, *20*. https://www.federalismi.it/nv14/articolo-documento.cfm?Artid=37234.

European Commission. (2018). *Communication from the Commission to the European Parliament, the Council, and the European Economic and Social Committee: A 'New Deal' for consumers*. European Union. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52018DC0183

European Commission. (2020, January 27). *Joint Statement by Vice-President Jourová and Commissioner Reynders ahead of Data Protection Day*. European Commission, Press Corner. https://ec.europa.eu/commission/presscorner/detail/en/STATEMENT_20_120

Garaci, I., & Montinaro, R. (2019). Public and Private Law Enforcement in Italy of EU Consumer Legislation after Dieselgate. *Journal of European Consumer and Market Law*, *8*(1), 29–34.

Granville, K. (2018, March 19). Facebook and Cambridge Analytica: What You Need to Know as Fallout Widens. *The New York Times*. https://www.nytimes.com/2018/03/19/technology/facebook-cambridge-analytica-explained.html

Hodges, C. (2019). Collective Redress: The Need for New Technologies. *Journal of Consumer Policy*, *42*, 59–90. https://doi.org/10.1007/s10603-018-9388-x

Information Commissioner's Office. (2019). *SCL Elections prosecuted for failing to comply with enforcement notice*[Press release]. https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2019/01/scl-elections-prosecuted-for-failing-to-comply-with-enforcement-notice.

Institute, E. L. (2018). - *International Institute for the Unification of Private Law (UNIDROIT*. https://www.europeanlawinstitute.eu/fileadmin/user_upload/p_eli/Projects/Unidroit_Materials/Trier_2018/WG_Parties_-_Draft_on_Collective_Redress.pdf.

Italian Data Protection Authority. (2019). *Cambridge Analytica: Facebook fined 1 million Euro by the Italian Dpa* [Press release]. https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9121506

Jančiūtė, L. (2019). Data protection and the construction of collective redress in Europe: Exploring challenges and opportunities. *International Data Privacy Law*, *9*(1), 2–11. https://doi.org/10.1093/idpl/ipy022

Malgieri, G., & Custers, B. (2017). Pricing privacy: The right to know the value of your personal data. *Computer Law & Security Review*. https://ssrn.com/abstract=3047257

Mann, M., Daly, A., & Molnar, A. (2020). Regulatory arbitrage and transnational surveillance: Australia's extraterritorial assistance to access encrypted communications. *Internet Policy Review*, *9*(3). https://doi.org/10.14763/2020.3.1499

Manokha, I. (2018). Surveillance: The DNA of Platform Capital – The Case of Cambridge Analytica Put into Perspective. *Theory & Event*, *21*(4), 891–913,. https://ora.ox.ac.uk/objects/uuid:15e74c10-225f-4bd7-b086-8e1fdb1b79e8/download_file?file_format=pdf&safe_filename=Manokha%252C%2BSurveillance%252C%2BAAM.pdf&type_of_work=Journal+article.

Money-Kyrle, R. (2016). Legal Standing in Collective Redress Actions for Breach of EU Rights: Facilitating or Frustrating Common Standards and Access to Justice? In B. Hess, M. Bergström, & E. Storskrubb (Eds.), *EU Civil Justice. Current Issues and Future Outlook* (pp. 223–254). Hart Publishing.

Nuyts, A. (2014). The Consolidation of Collective Claims Under Brussels I. In A. Nuyts & N. Hatzimihail (Eds.), *Cross-Border Class Actions. The European Way* (pp. 69–84). Verlag Dr. Otto Schmidt.

Pato, A. (2019). The Collective Private Enforcement of Data Protection Rights in the EU (2019. In L. Cadiet, B. Hess, & M. R. Isidro (Eds.), *MPI-IAPL Summer School*. Nomos. https://doi.org/10.5771/9783748900351-129

Privacy International. (2016). *The Global Surveillance Industry* [Report]. Privacy International. https://privacyinternational.org/sites/default/files/2017-12/global_surveillance_0.pdf

Trstenjak, V., & Weingerl, P. (2014). Collective Actions in the European Union—American or European Model? *Beijing Law Review*, *5*(3), 155–162. https://doi.org/10.4236/blr.2014.53015

Voet, S. (2017). 'Where The Wild Things Are': Reflections On the State and Future of European Collective Redress. In M. Loos & A. L. M. Keirse (Eds.), *Waves in contract and liability law in three decades of ius commune*. Intersentia. https://ssrn.com/abstract=2913010

Zuboff, S. (2019). *The age of surveillance capitalism: The fight for a human future at the new frontier of power*. Profile Books.

FOOTNOTES

1. Note that the recently adopted Directive 2019/770 on certain aspects concerning contracts for the supply of digital content also acknowledges the fact that personal data are used as counter-performance for 'free' digital services or for discounts on online products and services: Recital 67 and Art 3 (1).

2. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC, OJ L 119, 4.5.2016.

3. The doctrine of lis pendens is the basis for suspending or staying legal proceedings in light of other pending proceedings that involve the same or very similar parties, issues or relief. It is aimed at avoiding situations in which two equally final and enforceable decisions exist within the same legal system.

4. For instance, French legislation extends the scope of application of collective claims to data protection in Article 43ter French Data Protection Act of 6 January 1978. See Biard (2016).

5. According to the Austrian model of group litigation the claim is admissible if the basis for the claims is essentially similar and the claims have to refer to the same factual or legal question (Amaro et al., 2018).

6. Directive 2009/22/EC of the European Parliament and of the Council of 23 April 2009 on injunctions for the protection of consumers' interests (Codified version), OJ L 110, 1.5.2009.

7. European Commission Recommendation on common principles for injunctive and compensatory collective redress mechanisms in the member states concerning violations of rights granted under Union Law (2013/396/EU, OJ L 201/60, 26.7.2013).

8. Regulation (EU) 1215/2012 of the European Parliament and of the Council of 12 December 2012 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters (recast), OJ L 351, 20.12.2012.

9. Regulation (EC) 593/2008 of the European Parliament and of the Council of 17 June 2008 on the law applicable to contractual obligations (Rome I), OJ L 177, 4.7.2008.

10. Regulation (EC) 864/2007 of the European Parliament and of the Council of 11 July 2007 on the law applicable to non-contractual obligations (Rome II), OJ L 199, 31.7.2007.

11. Similar rules have been adopted in the Proposed Directive on representative actions for consumer claims in particular recitals (11a), (11ea) and (11f).