HELLENIC FOUNDATION
FOR EUROPEAN & FOREIGN POLICY

ΕΛΙΑΜΕΠ
ELIAMEP

Protecting data, ruling over the algorithm:
The Regulation Challenge for the European Union

EUROPEAN INSTITUTIONS AND POLICIES

George PAGOULATOS and Vasiliki POULA

October 2020
Policy Paper #40/2020

ELIAMEP |Policy Paper # 40/2020

Protecting data, ruling over the algorithm: The Regulation Challenge for the European Union

HELLENIC FOUNDATION FOR EUROPEAN & FOREIGN POLICY (ELIAMEP)
49 Vasilissis Sofias Ave., 10676, Athens, Greece
Tel.: +30 210 7257 110 | Fax: +30 210 7257 114 | www.eliamep.gr | eliamep@eliamep.gr

George PAGOULATOS
Professor of European Politics & Economy, Athens University of Economics; Director General, ELIAMEP

Vasiliki POULA
Law student, LSE; Junior Researcher, ELIAMEP

Summary

- The EU has put the goal of technological sovereignty on the agenda, as the world leader in Internet regulation. The enactment of the General Data Protection Regulation Act and the case law of the European jurisprudential landscape have propelled the fulfilment of this goal.
- In particular, the legal saga of Schrems II recently decided in the Court of Justice of the European Union has confirmed the regulatory capacity of the EU, by ruling that the transatlantic agreement to transfer data between the EU and US does not protect the privacy of European citizens in a way that satisfies requirements that are essentially equivalent to those required under EU law, and by ordering a halt to those transfers.
- While the European legal order has succeeded in recognizing data protection as a fundamental human right and has led the way in codifying the unknown territory of new technologies, there is still concern that the EU is handling the new challenges in a 'legalistic' way. In particular, we explore the persistent challenge of the exploitation of data in the commercial and political context and explain why microtargeting should become part of the EU's regulatory agenda.
- We conclude that the regulation of the algorithm is preferable to the ad hoc punishment of companies, so that the EU adopts a pre-emptive rather than a firefighting role. Ultimately, though, the EU has to be self-aware of the limits of regulation in an era of constantly evolving technology: finding ways to live with and encourage these technologies is equally important with finding ways to regulate them.

Introduction

Across the digital economy, Europe has been missing. The biggest tech companies are not based in Europe, and even European companies often run their businesses on infrastructure from non-European-based companies.

Yet, Europe has put the goal of technological sovereignty on the agenda. The EU might not be capable yet of technological sovereignty in producing technology, but it can further establish itself as the world leader in Internet regulation, especially when it comes to data and privacy, seeking the golden mean between regulation and connectivity. Will this pursuit be accompanied by an effort on the part of the EU to nurture its own tech ecosystem? It remains to be seen.

What we *can* say with certainty, is that the EU has managed to reposition data protection laws from the periphery of legal consciousness to the centre of intensive legal and media publicity. And it has done so, primarily, through the enactment of the General Data Protection Regulation Act (GDPR) and its related case law. We focus on the legal saga of *Schrems.* While such regulation is indeed necessary, we highlight that there is a tendency for EU data protection law to focus on legalistic mechanisms to protect data transfers rather than on protection in practice, and particularly, with regards to the exploitation of data and microtargeting in the commercial and political context.

Regulation of data transfers needs to go beyond formalistic measures and legal fictions, so that the EU adopts a pre-emptive rather than a firefighting role. And, perhaps, we should start thinking of solutions that go beyond the digital ecosystem to tackle the problems within it.

Data protection through legal means

The European Union has celebrated the European Data Protection Day on the 28th of January since 2006. On that very day, in 2014, Viviane Reding, Vice-President of the European Commission, responsible for Justice, Fundamental Rights and Citizenship, spoke on "A data protection compact for Europe" arguing that "data collection by companies and surveillance by governments are connected, not separate". She went on: "Data should not be kept simply because storage is cheap. Data should not be processed simply because algorithms are refined. Safeguards should apply and citizens should have rights."

Those statements can be read as a precursor to the GDPR, EU law's regulatory tile in the mosaic of data protection and privacy. The GDPR, as implemented since May 2018, has two unique elements.

Firstly, through the GDPR, the EU enshrines data protection as a fundamental human right (Recital 1). Article 8(1) of the Charter of Fundamental Rights of the European Union and Article 16(1) of the Treaty on the Functioning of the European Union (TFEU) also provide support for the assertion that everyone has the right to the protection of personal data concerning them.

Secondly, the GDPR also applies to data controllers and processors outside of the European Economic Area (EEA) if they are engaged in the "offering of goods or services"

(regardless of whether a payment is required) to data subjects within the EEA, or are monitoring the behaviour of data subjects within the EEA (Article 3(2)) – regardless of where the processing takes place. This has been interpreted as intentionally giving the GDPR extraterritorial jurisdiction for non-EU establishments if they are doing business with people located in the EU.

"The GDPR acknowledges that it would make no sense for the EU to assert fundamental rights for EU nationals, or a particular geographic region, but not for anyone else."

The GDPR acknowledges that it would make no sense for the EU to assert fundamental rights for EU nationals, or a particular geographic region, but not for anyone else. Given the open nature of the internet, there had to be one data protection act to rule them all. It was a warning to companies everywhere that they would not evade the reach of European law simply by being located outside the EU.

The extent to which the EU's vision as global rule maker in the context of data regulation was to be fulfilled is constantly tested judicially in the European public order. It should be recalled that protection of fundamental rights in Europe takes place both under EU law (and its Charter of Fundamental Rights) interpreted by the Court of Justice of the European Union (CJEU), as well as the human rights instruments of the broader Council of Europe (which includes both the 27 EU member-states, as well as 20 other European States), on the basis of the European Charter of Human Rights (ECHR), as interpreted by the European Court of Human Rights (ECtHR).

"The extent to which the EU's vision as global rule maker in the context of data regulation was to be fulfilled is constantly tested judicially in the European public order."

Consequently, one would expect that the dialogue of European judges would be particularly rich and constructive regarding the assessment of the compatibility of data protection laws with fundamental rights, with the CJEU referring to the case law of the ECtHr and vice versa. However, this expectation holds little descriptive power over the status quo, a reality that perhaps suggests a divergence of views between the two courts. But we focus on the recent landmark *Schrems II* case of the CJEU.

In brief, the legal saga goes back to 2014 when privacy activist Max Schrems brought a complaint in Ireland against the Irish Data Protection Commissioner. He argued, following the Snowden revelations, that the privacy of European citizens could not be guaranteed if their data was sent to the US, given the evidence of widespread eavesdropping by the country's National Security Agency (NSA), and the fact that the US legal system only protected the rights of US citizens. This initial complaint led to the overturning of the EU-US Safe Harbour arrangement that Facebook had joined and which the Commission had found in a decision of 2013 to provide an adequate level of data protection. In particular, in 2015, the CJEU invalidated the adequacy decision, and held that an adequate level of data protection requires that third country law be "essentially equivalent" to EU law.

Schrems then alleged that Facebook's use of the standard contractual clauses for data transfers approved by Commission Decision 2010/87 (referred to here as 'the SCCs') could not provide a valid legal basis for transfers to the US, in part because Facebook is obliged to make the personal data of its users available to US government authorities in the context of their surveillance programs. The examination of these allegations also dealt with US law and practice regarding surveillance and the level of protection provided by the EU-US Privacy Shield, which was designed as a successor to the invalidated Safe Harbor and which was found to provide adequate protection in Commission Decision 2016/1250.

On 9 May 2018, the Irish High Court referred eleven questions to the CJEU. The most important aspect of the CJEU's recent judgement (July 2020) in relation to Facebook regulation was that the EU's top court ruled that the transatlantic agreement of Privacy

Shield, used by thousands of companies to transfer data between the EU and US, including Facebook, does not protect the privacy of European citizens "in a way that satisfies requirements that are essentially equivalent to those required under EU law". The ruling does not immediately end such transfers but requires data protection authorities (DPAs) in individual member states to vet the transfers of any new data to make sure people's personal information remains protected according to the EU's data protection laws (GDPR). Thus, the court has clearly told the DPAs that they can no longer bury their heads in the sand, and that instead, they have to enforce the law, i.e. the GDPR.

Nevertheless, the court upheld the use of SCCs, i.e. individual legal agreements covering how data will be treated, to transfer personal data between Europe and US, allowing companies to seek specific consent from users for data to be exported. However, companies will now have to carefully analyse whether their SCCs are sufficient to ensure that data moving overseas are treated in line with the EU's GDPR. The judgement has made it clear that companies, in general, and Facebook, in particular, cannot justify using a 'tick box' exercise of putting SCCs in place.

"…the Commission would also continue to push the US administration to accelerate work on an American federal privacy law that would be equivalent or similar to the GDPR."

In response to the judgment, Brussels said it would accelerate its work on modernising SCCs to ensure they can handle the vast flows of private data outside the EU. After all, data flows between Europe and the United States are an integral part of the European economy and of the day-to-day lives of millions of European consumers, and the SCCs are the backbone for many of those data transfers. But at the same time, Vera Jourova, EU executive Vice-President in charge of values and transparency, said the Commission would also continue to push the US administration to accelerate work on an American federal privacy law that would be equivalent or similar to the GDPR.

When Europe enacted GDPR, the world's toughest online privacy law, hopes and expectations were high. Now, many see it struggling to fulfil its promise with Europe's rules being a victim of a lack of enforcement, poor funding, limited staff resources and stalling tactics by the tech companies. Penalisations are too few (only Google has been subject to penalty), too little (e.g. Google was fined 50 million euros, equivalent to about one-tenth of what Google generates in sales each day) and too late, leaving regulators at risk of fighting yesterday's battles. The cases could drag for several more years as a result of court appeals. And with limited financial resources, critics argue, the authorities are inclined to be overly cautious and avoid more complex cases.

"…the judgment of the CJEU in Schrems is a victory of GDPR and of the EU's regulatory capacity."

Certainly, the judgment of the CJEU in *Schrems* is a victory of GDPR and of the EU's regulatory capacity. It remains to be seen if the case will result in more harmonized global data protection standards enabling the creation of solid legal instruments for future international data transfers or, instead, to a limitation of free data flows and data localization solutions. Berlin's Data Commissioner's support of the latter option, calling for data currently stored in the US to be relocated to the EU, was definitely an interesting development. But we can say confidently that the EU has assumed a role as the global regulator of the digital sphere, with its case law providing a definitive reference point against which the challenges presented by EU-US data transfers can be addressed into the future, bringing certainty to bear in an area that has been beset by uncertainty for some considerable time now.

Data- and algorithm-related concerns beyond the ambit of the law

While the European legal order has succeeded in recognizing data protection as a fundamental human right and has indeed established itself as the regulatory leader on the digital sphere, this does not mean that everyone has suddenly grown complacent of digital platforms' growing interference with data.

There is something unique about data – the simple rule that the higher the consumption of a good, the lower its reserves become, does not hold for them. Data does not run the risk of becoming scarce. Not in the sense that we might have endless data – lack of efficient compression algorithms means that a data shortage could be imminent in the next decade, unless large and costly data centres are erected. But in the sense that one piece of information about someone can be used again and again by different stakeholders, without it losing its value. The economic and political implications of the infinitely usable nature of data are of great importance and of potentially great value. And what is the main threat? Microtargeting. This means that the danger lies in the platforms' unique capacity of launching ultra-successful campaigns through direct marketing datamining techniques that involve predictive market segmentation.

"…one piece of information about someone can be used again and again by different stakeholders, without it losing its value."

The two troubling applications of 'microtargeting' are those in the commercial and the political context, with the common denominator being the weakening of the user's free will against Facebook's overwhelming power. Both of those threats are widely tackled in public discourse and are often treated with a grain of sentimentalisation – as was the case in the recently released documentary *The Social Dilemma*. This paper attempts to assess the two parameters in a non-manichaeistic way, and by no means do we purport to be the Cassandras of the debate.

A. The commercial context

An adequate explanation of what dangers lurk through microtargeting in the commercial world is reflected in the concept of 'surveillance capitalism'. This – gimmicky – term was coined by Shoshana Zuboff to describe the new paradigm that our economic order enters, as companies increasingly claim the human experience on social media as products. The justification is simple: 'if you are not paying for the product, then you are the product', and this hypothesis makes perfect sense for new media, whose business model lies in surveillance: users cheerfully become part of the medium's exciting vision of a more connected world, enabling the providers of this vision to monitor the behaviour of those users in astonishing detail – often without their explicit consent – and sell it to whoever is interested, or in fact, to whoever pays more.

"An adequate explanation of what dangers lurk through microtargeting in the commercial world is reflected in the concept of 'surveillance capitalism'."

What exactly is sold? The more 'vanilla' edition of the argument is that the users' attention is the product being sold to the advertisers. The more serious allegation is that it is the gradual, slight, imperceptible change in the users' behaviour and perception that is the product. Additionally, new media can sell certainty in an unprecedented way – advertisers know that if they launch an ad through Facebook, it will be extremely successful. Thus, one could even reach the conclusion that markets trade in human futures.

An advantage of the new revolutionizing advertisement techniques would be the provision of ad opportunities to small and medium-sized enterprises, which in the past would not have had the resources for newspaper ad space or a slot for a TV commercial. And not only do those SMEs have access to advertisement, they can also ensure that their ads are efficient and effective. This has also lowered the barrier to entry for start-

ups, by enabling them to reach a very specific group of potential users or customers without spending a fortune. 'Microtargeting has democratised advertising', they say in Silicon Valley jargon, but let's not get too ahead of ourselves. The big still get bigger, but now the small have more chances to play the game.

B. The political context

The dangers that Facebook poses on our political communities affect a number of their aspects. A primordial dilemma that arises is whether digital platforms act as tools to promote democracy or as a mechanism of auctioning our democracy off to the highest bidder. The supporters of the latter opinion justify their thesis through three observations.

I. Multiplying fake news

Firstly, modern media have multiplied the possibilities of the (cross-border) dissemination of marginal, uninformed voices. In the 20th century, the public sphere was formed around mass media. A combination of public scrutiny and large media conglomerates prevented outrageous extremes and largely restrained the terms of the game. There have always been the yellow press and vulgar "reality" shows. Their audience was relatively homogeneous, but the multiplicity of interaction and the socialization of the believers, was absent; an unbalanced conspiracy theorist had difficulty meeting interlocutors. The internet solved this problem. It brought together people with outrageous, marginal views, who created communities and groups of like-minded people, within which the confidence and dynamism of marginal views is multiplied. Erratic, uneducated, paranoid people acquire around them a community that expands the reach and virality of their beliefs.

"It brought together people with outrageous, marginal views, who created communities and groups of like-minded people, within which the confidence and dynamism of marginal views is multiplied."

The great achievement of the democratization of information has, however, come with abolishing the filters that once prevented false information from gaining access to the public sphere. Anyone can post the most outrageous lie, next to fact-checked news by reputable organizations that operate according to strict journalistic ethics. It is becoming increasingly difficult to evaluate information on the internet – a truly demanding challenge for the uninitiated. And this becomes even more problematic due to algorithms' capacity to prioritise information for their users and to perform content moderation. Social media algorithms take the reins of determining which content to deliver to their users based on their behavior – for instance, Facebook or Twitter might put posts front-and-center in one's feed because those posts happened to be popular with their close friends or within the community that is in geographic affinity. This means that the algorithm has the power to not only bring together believers of fake news, but also to expose more people to fake news. The potential for the abuse of data by the platforms' algorithm was raised by the President of the Commission in her 2020 State of the Union Address: "We want a set of rules that puts people at the centre. Algorithms must not be a black box and there must be clear rules if something goes wrong". Wide-spread AI fact-checking could be a solution.

"Wide-spread AI fact-checking could be a solution."

But even statements that could be debunked in a seemingly straightforward manner – for instance, the now-infamous Brexit campaign claim that the UK would save £350m per week by leaving the European Union – present a thorny challenge for automated verification. Two risks lurk. On the one hand, there is bias – our stereotypes, prejudices, and partialities are known to affect the information that our algorithms hinge on. In the same way that algorithmic bias could ruin a self-driving car if there's not enough night-time data, a prejudice bias could unconsciously reflect personal political or ideological

convictions, for instance, on fact-checking. On this front, we can only hope for more sophisticated deep learning mechanisms.

"…there is the dilemma of balancing free speech and access to accurate information."

On the other hand, there is the dilemma of balancing free speech and access to accurate information. The argument is that unless they cross specific legal red lines – such as those barring defamation or libel – fake news stories are not illegal, and as such, regulatory bodies are not legitimate prohibiting or censoring them. The basis for such an argument is often found in Article 10 of the ECHR (freedom of expression), the US Constitution First Amendment and international free expression safeguards. Nevertheless, the superficial protection that free speech rhetoric offers to fake news does not nullify the danger it poses for open discourse, freedom of opinion, or democratic governance. The rise of fraudulent news and the related erosion of public trust in mainstream journalism pose a looming crisis for free expression. The blatant reversal of the truth, as in post-truth Trump accusing the serious factful mainstream press as "fake news", only adds insult to injury. Usually, free expression advocacy centres on the defence of contested speech from efforts at suppression, but it also demands steps to fortify the open and reasoned debate that underpins the value of free speech in our society and our lives. The championing of free speech must not privilege any immutable notion of the truth to the exclusion of others. But this does not mean that free speech proponents should be indifferent to the quest for truth, or to attempts to deliberately undermine the public's ability to distinguish fact from falsehood.

"The rise of fraudulent news and the related erosion of public trust in mainstream journalism pose a looming crisis for free expression."

The European Democracy Action Plan, to be unveiled in late 2020, represents the next step in the EU's regulatory fight against fake news, in the spirit of countering the aforementioned observations.

II. Polarizing content

If the reproduction of fake news is the first symptom, the second one would be militancy. An internal Facebook study documented that this medium's algorithms exploit the human brain's attraction to divisiveness and polarization. In his fascinating book "Thinking, Fast and Slow", Daniel Kahneman distinguishes two "systems" of mental function: "fast" thinking works automatically, spontaneously, uncritically and impulsively. "Slow" thinking requires effort, rational assessment and strategic reasoning. "Fast thinking" is the function that flourishes on social media, where reaction is decisively influenced by the impulse, the image, the context, the group dynamics, the echo chamber, the mass. Without filters and balances, "fast thinking" spreads false and divisive speech like dry grass spreads fire. Then social media become a weapon for conspiracy theorists and demagogues.

"As free markets require regulation to protect fair competition and deliver the goods, so does pluralism require rules."

Democracy needs the resistance of "slow thinking". It requires exhaustive dialogue, negotiation, the seeking of consensus, compromises. These are the ingredients of liberal democracy, which becomes devoid of meaning when arguments are replaced by lies and insults, and the understanding of the other's position by mob e-lynching and the "cancelling" of ideological opponents. Liberal pluralism has always been based on a normative judgement disguised as an optimistic expectation: That if you allow all views free to express themselves, to compete, to clash with each other, the truth will emerge and prevail. This has not always been vindicated by reality, as a plurality of examples including Trump and Brexit serve to remind us. As free markets require regulation to protect fair competition and deliver the goods, so does pluralism require rules.

III. Creating echo-chambers

But a third, and perhaps even more concerning reality that hinders our democracies is neither the magnifying effect that Facebook has on fake news, nor the divisive rhetoric, but rather its contribution to the creation of echo-chambers.

Before the House Financial Services Committee, Alexandria Ocasio-Cortez asked Mark Zuckerberg: Would she be able to run advertisements on Facebook targeting Republicans in primaries saying that they voted for the Green New Deal? His answer was probably yes, since they are not calling for violence or risk imminent physical harm, or voter or census suppression, indirectly referencing the First Amendment that protects freedom of speech. Asked further, he added: "Yes, in most cases, in a democracy, I believe that people should be able to see for themselves what politicians, that they may or may not vote for, are saying or think so they can judge their character for themselves."

"The public sphere creates an informal system of checks and balances, and thus, of accountability; these notions that are lost in the echo chambers of digital platforms."

And herein lies the problem. Politics used to be part of the public sphere. And when something is said in public, people may judge by themselves, but they also judge with others. When a piece of information is displayed to the public, we assume that if it is incorrect, illegal or fake someone with the knowledge or the interest or incentive to debunk it (e.g. the party that is being damaged by it or the authorities if it violates a law) will do so. We rely on public scrutiny and public discourse to counter the asymmetry of information and the asymmetry of power between the broadcaster and the recipients of a message. The public sphere creates an informal system of checks and balances, and thus, of accountability; these notions that are lost in the echo chambers of digital platforms. Due to microtargeting, there is no one to jump in to doubt the accuracy of a message, simply because that message would not have been sent to anyone, who would care to react or who would have the knowledge to react. Therefore, microtargeting creates an asymmetry that strongly favours the broadcaster of the message and puts the recipient in disadvantage.

Reform or regulate?

In an ideal world of benevolent market participants, self-regulation should do the job. It is true that digital platforms have taken steps to self-regulate. But self-regulation is determined by a "we know we have more work to do" mentality, an idea that seems to be repeated by platforms once found at fault – for instance, such rhetoric was brought up both after *Schrems II* and after the #StopHateForProfit advertising boycott campaign launched against Facebook. The phrase is both a promise and a deflection. It is a plea for unearned trust – *give us time, we are working toward progress.* And it cuts off meaningful criticism – *yes, we know this isn't enough, but more is coming.*

"Platforms frequently use unfathomably vast amounts of content as an excuse for inaction. But this defence is also an admission: they are too big to govern responsibly."

Platforms frequently use unfathomably vast amounts of content as an excuse for inaction. But this defence is also an admission: they are too big to govern responsibly. There will always be more work to do because Twitter's or Facebook's design will always produce more hate than anyone could monitor. How do you reform that? Or an even more pertinent question perhaps – can you reform that or do all signs point to a system beyond reform?

The EU has opted for the path of regulation. And indeed, the EU's steps towards regulating digital ecosystems are welcome, as it is, indeed, true that we cannot rely on self-regulation for something so powerful and so (potentially) dangerous. The demand

for stricter control and harsher sanctions over tech companies is welcome, but those measures would always fall short of seeing the big picture. Instead of trying to curtail companies, the EU should take one step back and try to regulate the way in which emerging technologies are applied by those companies, i.e. the constituent parts that form our digital landscape, as it has attempted to do so far. Otherwise, the risk of sporadic, incoherent and inconsistent policy-making on an ad hoc basis lurks. The case of *Schrems* has set a good precedent, but other fronts of this war remain to be fought.

Tech companies might resist, but negative externalities will always justify EU regulatory initiatives. A recent example of platforms and regulators reaching this equilibrium comes from Facebook's threats to leave Europe due to proposals for new data-sharing regulations. Complying to those new regulations would be complicated, restrictive, and expensive. But by a complete pull-out, Facebook would lose a lot of money and market share. As such, the most likely scenario would eventually see Facebook forced to establish EU-only data centres.

"…we have to be aware of the limits of the regulation effort. Perhaps we have to face the reality that no matter how much we regulate, something will be lacking."

But at the same time, we have to be aware of the limits of the regulation effort. Perhaps we have to face the reality that no matter how much we regulate, something will be lacking – it will always be the case that another platform will emerge in a different jurisdiction or a new technology will make its appearance, rendering the legal regulatory regimes outdated and redundant. Finding ways to live with these technologies, and encourage their development, is equally important with finding ways to regulate them. As such, policies that could indirectly strengthen collective immunity against the negative implications beyond the digital world should be welcome. Investing in public education is a good first step, particularly when it comes to demonstrating the difference between passionate argument and hate speech, heterodox views and public paranoia, good journalism and fake news trash. Admittedly, easier said than done.