BRUSSELS SCHOOL OF GOVERNANCE

ECONDIS STUDENT PAPER SERIES

2022

INSTRUCTOR:
Prof. Dr. Sven Van Kerckhoven

TITLE OF PAPER:
Digital Economy in Europe, Privacy or Competitiveness?

NAME OF STUDENT:
Félix Gerling

This paper series consists of student papers drafted in the framework of the course ECN202: The European Economy, offered at the Brussels School of Governance.

The course is offered with the support of the Education, Audiovisual and Culture Executive Agency of the European Commission as a Jean Monnet Module, entitled 'ECONDIS: The Economics of European (Dis) Integration' under the Grant Decision No. 2019-1814/001-001.

Other academic publications originating from the project are:

Van Kerckhoven, S. (2021). Post-Brexit Leadership in European Finance, Politics and Governance, 9(1), pp. 59-68.

Van Kerckhoven, S. and Odermatt, J. (2021). Euro clearing after Brexit: shifting locations and oversight, Journal of Financial Regulation and Compliance, 29(2), pp.187-201.

Van Kerckhoven, S. (2021). The impact of Brexit on the European single financial market, Brexit Institute News, Dublin City University Brexit Institute, 27 April 2021, available at: http://dcubrexitinstitute.eu/2021/04/the-impact-of-brexit-on-the-european-single-financial-market/

Van Kerckhoven, S. (2021). Brexit heralds a bleak future for the City of London, LSE Brexit Blog, 3 March 2021; available at: https://blogs.lse.ac.uk/brexit/2021/03/03/brexit-heralds-a-bleak-future-for-the-city-of-london/

Co-funded by the Erasmus+ Programme of the European Union

Policy Paper: Digital Economy in Europe, Privacy or Competitiveness?

Brussels School of Governance

-

European Economy

Félix Gerling

Executive Summary

The research conducted in this paper is to know how the European Union can deal with its digital legislation and still be competitive in terms of technological innovation. The research is focused on two aspects linked directly to the European economy. On first, I focused my research on digital privacy, what it means for Europe compared to other nations and how it affects its citizens.
I found that digital privacy in Europe is the strongest in the world due to its long process of development of its General Data Protection Regulation (GDPR) implemented in 2018. Even though it is a good regulation for European citizens, the EU has no central authority organ to sanction companies that don't respect the GDPR, the Data Protection Authority (DPA) belongs to each nation.
Another finding is that the EU might have some difficulties trading with other nations due to the GDPR because the standards of privacy are so high that foreign companies struggle to bring themselves up to speed.

This first step brings me to the second aspect I focused the research on: the competitiveness that results from the GDPR. How it affects businesses, innovation and how it is perceived by the other leaders in the digital field.
The findings on this aspect are that data trade between EU and foreign countries is difficult and it is a brake for development and innovation in the AI field. This technology is processing a lot of data and it is a way for AI companies to make a profit out of it, so GDPR decrease this benefit and makes Europe a less attractive land for innovation. However, some companies like Microsoft adopted the GDPR for their entire network. This is called the "Brussels Effect" when a European regulation is good, and companies implement it for their whole business.

Introduction

The European Union (EU) is the most advanced organization in the world in terms of digital privacy regulation thanks to its GDPR. For the citizens who go online every day, it doesn't change a lot except that they must give their accord to accept cookies or not, on every website they go on. For companies, however, it is a game-changer because the legislation is so complex that they must hire lawyers and jurists to adapt to it. The 21st century is marked by its ongoing technology innovations like Artificial Intelligence (AI) and Big Data. Data needs to be massively collected to feed progress through the famous cookies and countless data sales to third companies for unknown usage. The GDPR is exactly made to avoid any companies in any domain to use these data without control to create profit. It means that it prevents companies from selling them to third companies and protects the consumer from privacy intrusion. Recently, a company called IAB Europe that sells data for real-time bidding was sued for its Transparency & Consent Framework (TCF) (Marsac 2022). The bids are not made by people of course, it is an automatic process involving AI, but the data are sold to tier company. Alphabet (Google) and Meta (Facebook) that are both data brokers started to decrease their sales of data in huge quantity to tiers companies that have no choice but to accept it. The article of La Libre Belgique argues that they will better process the data to make them completer and more qualitative rather than selling the quantity. It means that data will be more expensive.

This measure has been well received by the Europeans because if we trust a BBC World Service poll from 2009 to 2010, it reveals that in France and Germany, approximately 75% of the people asked said that the internet was not a safe place. Furthermore, nowadays, technologies have evolved, people have even less digital background to understand how AI works or fear losing their job, resulting in a fear of AI. Currently, the EU is not the leader in terms of investments in new technologies but in the digital industry, it is. Other nations sometimes struggle to make deal with the EU because the GDPR is so constraining that it is not attractive. Therefore, in a period where privacy is recognised as a human right but where innovation is a gamechanger for the future of Europe and the world, the question this paper is attempting to answer is: "*How can the EU balance privacy and competitiveness in the digital field and be a leader in the digital economy?*".

The first part of this work is the literature review that gathers a dozen sources. Then, it will lead to the analyse of these sources in order to find limitations linking them to theory and illustrated with empirical examples. The conclusion comes to wrap up the main arguments and answer the research question.
The main argument of this paper is that Europeans have the chance to evolve in an environment that promotes their basic human right to digital privacy more than any other country and due to the Brussels effect, we can hope that a great part of the world will adopt soon or late the same regulation and that will result in a more and more competitive European Union. On one hand, privacy should be improved but on the other hand, it should not be too improved to not hinder innovation too much.

Literature review

Privacy

Wylde et al (2022), explain that the GDPR has the function to verify how businesses, states and organisations utilise personal data and make sure there are no bad intentions in the treatment of personal data. To do this, any organism using personal data must respect at least the eight basic objectives of the GDPR. That is to say: be responsible for handling and processing of personal data; data acquisition must be lawful; acquisition must be fair, the acquisition must be accurate, data must be up to date; data must be kept safe and secure; data cannot be transferred outside the European Economic Area.

As explained in the work of Bygrave (2010), our first aspect, privacy is already evolved among European members in terms of legislation, due to the GDPR. Data flows are regulated and controlled; citizens are safe in regard to other nations. But we do not live in a world without interaction between nations, in cyberspace, it is the same. Therefore, it is legitimate to wonder what other nations' companies do with EU citizens' data. In Europe, the Council of Europe (CoE) has adopted the GDPR as a standard for every member which is a good thing already. The Association of Southeast Asian Nations has also voted for a GDPR like regulation recently that promotes a digital relationship with the EU.

In 2019, the EU took another dimension in regard to data protection. The Convention 108+ of the CoE put an emphasis on AI and Big Data. The Convention 108+ is the data protection convention of the Council of Europe organized in 2018 in Strasbourg. However, this text was criticized because of its lack of Big Data regulations. Indeed, De Hert and Sajfert (2019) expose the fact that the GDPR doesn't pay attention to the Big Data, data protection law and Big Data technologies being completely heterogeneous. On contrary, the two authors explain that the EU would have endorsed Big Data outside its laws of data protection.

The 2017 Big Data Guidelines recognize the world as a Big Data world that cannot be denied. Those companies are said to be a source of progress and innovation for society. But none of the risks of Big Data is explained or restricted in the convention 108+ and the GDPR. And this resilience depends on the success of the soft law guidance (De Hert and Sajfert). However, in other countries like China, data collection and use are completely different because the regime of Xi Jinping settled a logic of surveillance capitalism that gives no right to privacy to its citizens (Aho & Duffield).

As said by Hu (2019), the GDPR is the most complex and finished legislation of the EU in terms of data protection. But it is also made to continue the trade of data within the EU to not hinder the data economy. According to De Hert & Papakonstantinou (2021), this is the role of the DPAs to advise and help companies to make good choices to avoid financial penalties.
However, some DPA might have a biased opinion on whether to choose the data protection or the data economy because it is a national competence.

Economy

For the digital development of its economy, the EU Digital Compass plans to give wide access to 5G, develop the first quantum computers and double the share in global production while respecting its climate engagement. For the ordinary mortal, the EU wants everybody to have an internet connection and have a medical record online. So, in terms of development, the EU will increase its investment and support innovation programs while keeping digital privacy a priority with the GDPR (European Commission). In theory, Aho & Duffield (2020) explain that the GDPR is expected to provide economic benefits due to the harmonization of the legislation and it is part of the EU's single market. It also means that data operations are oversight by governments, and this is a reason why it has been feared that companies would prefer to delocalize in the US or other countries where no government can control operations as much as the EU does.

Ezraki (2018) argues that the shift toward a digital economy has already stimulated the market dynamics and let the development of multi-sided markets. It brings uncertainty and competitive pressure to the market to self-correct. The author says that the new digital businesses raise new questions about the optimal use of competition laws in the accumulation of data and the use of big analytics. To answer this question, he explains that the protection of an "effective competition structure" is important for consumer welfare and the economy. That could help the EU to have more power through competition agency for actions distorting competitiveness. This could imply a more effective consideration of effects on the digital landscape. The author argues that the continuously increasing significance of data in shaping markets and driving their development proves its relevance as a parameter in the assessment of markets and possible distortion of competition. Furthermore, the upstream effects' consideration might offer the EU a better perspective of practices that can negatively impact the consumer at the end of the chain. Within the EU it means that data flow is much freer and gives opportunity

In regards to the digital economy, many regions of the world have already implemented some laws for data protection. For instance, we can find in trade organizations rules and laws about the protection of data like the Asia Pacific Economic Cooperation. Even though it is only "soft laws", that is to say, laws broad enough to be ratified by many states and they also might have a great political and commercial impact on those who ratify them. The goal of exporting jurisdiction abroad is important for the EU because one of the GDPR's criticism was that businesses based on data flow were negatively impacted. Therefore, having economic partners with the same data protection level would revitalize the business of data in Europe. According to the article by Bygrave (2010), the EU Directive became a trendsetter in shaping national data protection regimes but also an international instrument for free data flow.

However, world industries have come into contention because of the differences in norms and values of each region shaped by the different political regimes, Europe included. The article of Aho & Duffield (2020) explains that China's model of digital privacy is the Social Credit Score (SCS) which gives no privacy to citizens but gives a lot of opportunity for technological innovation. But Europe needs to be competitive and needs to accept international companies on its territory. So, the use of European data is an important matter (Aho & Duffield). According to Hu (2019), it seems that the EU deliberately choose to not include strong and detailed rules about Artificial Intelligence in the GDPR because it is an

enormous source of innovations and economic benefits. Using very precise words would have ruined the development and the possible economic repercussion it has.

Analysis

So, we understand that there might be a correlation between digital privacy and economy and the balance between the two of them result in a more or less dynamic innovation rate. The innovation comes from companies within the European Union or outside of it. It means that the EU needs to make agreements with other countries like the USA and China which are the two biggest investors in AI. Therefore, the different countries must find a bilateral agreement for trade liberalization of data. The issue is the different positions related to data privacy. Companies using AI and collection of data must respect the GDPR and it costs them money in lawyers, production, design etc.

According to the paper by Schwartz (2019), the Brussels effect is the impact that European legislation have on multinational corporations and that no foreign country has adopted the GDPR as it is. But democratic countries with a high and medium GDP tend to develop GDPR like legislation that can be part of the Brussels effects. In 2018, the State of California adopted a data regulation, the California Consumer Privacy Act that doesn't harm the many high-tech companies present there. There is a reason for that, and it is the Brussels effect. For instance, Microsoft adopted the GDPR for the European market on a first time and then expanded it to all its markets. It would be more expensive to withdraw from the European market than adapt its products and services and stay in it. So, in a way, the GDPR is not a constraint for the development and innovation of high-tech companies in Europe since some of them already applied it.

But we missed a variable in the equation. Indeed, the size of a corporation determines its survival chances with new legislation. To support this argument, I interviewed a cyber security expert for Nokia. According to him, companies like the one he works for have a lot of funds and this is very important when a whole set of products must be modified to comply requirements of GDPR. The cyber expert is also engaged in a startup he co-founded and deals with GDPR. He explains that they don't have a lot of funds, but they have the chance to be financially supported by the EU and it gives them the opportunity to get lawyer services to meet GDPR requirements. However, he explained in the interview that without this help, his projects would be born dead because GDPR is so complex that they have to engage a lawyer to not be sanctioned by its country DPA.

The choice of a European country to develop technology business is an important variable as well because the Data Protection Authority is a state competence, and every state has its preference between privacy and competitiveness. It creates somehow a not fair internal market because to have a fair internal market, the EU is committed to a common regulatory framework to prevent one company or country from gaining a competitive advantage by getting rid of regulations. This is not the case for DPA because each European country has its own autonomous one that follows the GDPR basic articles. However, according to Botta & Wiedemann (2019), the GDPR has left some room for interpretation due to its vague choice of words. That means that the DPA of a country can interpret an article differently than his neighbor. And this is the reason why so many big companies utilizing data choose countries like Ireland or the Netherlands, their DPA being more interested in economics rather than privacy, in parallel with their taxation strategy. We can see that in figure 1 in the appendix. It

shows the average amount per fine the DPA give to companies. Ireland and the Netherlands have the lowest corporate tax rate in the EU and that is the first reason why companies like Ryanair and Google settle their European Head Quarters there. The second reason according to Vincent Manancourt, writer for Politico, the Dutch DPA is seen as a strong and strict actor in the fight against privacy intrusion at the European level, but it is not what the facts show. The same article explains that the director of the Dutch DPA, Aleid Wolfsen, had no data protection background, and due to understaffing problems, the Dutch DPA is very laxist. It means that companies have more opportunities to break the GDPR and thus, have fewer risks of fines.

Recently, President Joe Biden and the president of the European Commission Ursula von der Leyen agreed in principle on new transatlantic data flows. But what does it mean for the data economy? Well, according to the sayings of Nick Clegg, President of global affairs for Facebook, the trade flow agreement will provide numerous opportunities for business development. Kent Walker, Google's president of global affairs and a homologue of Nick Clegg, also welcomed the agreement. So, for big data companies, it is good news. But is only good news for American firms because companies like Huawei or other foreign high-tech companies don't have the regulation structure that corresponds to the European one.

The case of Huawei and its 5G is a very big concern for data privacy. Indeed, according to Rühlig & Björk (2020), the giant Chinese high-tech and its offer of 5G service is controversial because the company is close to the Chinese government which represents a threat on many levels to Europe. The first one is digital sovereignty. Since Huawei will be in a position of force regarding the use of data provided by the activation of the 5G service, the EU might not be able to make sure data won't be used due to its lack of data agreement with Xi Jinping's government. Then, the level of mistrust between the EU and China is so high that European countries fear industrial espionage and even political sabotage. The final point is that the Digital Compass for 2030 describe the goals of the EU and one of them is a massive investment in AI and technologies to find a secured path for digital independence. And, according to Rühlig & Björk (2020), China's Belt and Road Initiative targets Europe by controlling flows of goods, services and data, increasing its dependency.

Conclusion

So far, Europe has a leader role in the exportation of regulation concerning private data protection, the so-called "soft laws". The role of the European Union in the implementation of rules in the context of the Council of Europe for data protection is a proof of that and other international organizations like the ASEAN have the same strategy It means that the strategy of the EU to bet on better digital privacy than his economic partners was a good idea and won't be that much negative in the future because more standardized rules, based on GDPR means more partners and an easy data flow. Artificial Intelligence has an economic potential well known but not fully achieved so it is important to not undermine it too much.

The differences in structures for the protection of data and market fairness at the national level within the EU are, however, a brake for development. A harmonization must be done to better export the norms and values abroad. Even though the EU has already exported some rules with the Convention 108+, the exportation of the structure of regulation is equally important. Then, it is important for the EU to increase its investment in AI and high technology development through fair competition market rules, but it is also important to find a good

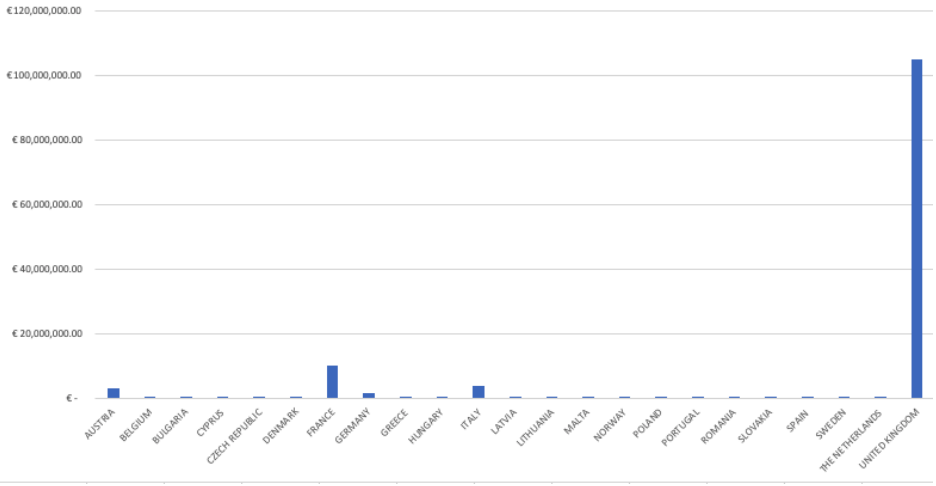
balance between fair competition market rules and data protection. This can be done with the harmonization of the DPAs. That is to say, giving the EU the competence to implementation of the GDPR. Or the creation of a European regulator that studies and evaluates each case of transgression. This regulator should also have the possibility to take control and financially reprimand companies in case of non-respect for data protection.

Finally, Step by step the EU is able to make other nations adopt its norms and values for the digital economy. However, the interview of the cyber security expert has ended with these words: “Exporting the ideas of the GDPR is complicated but having the whole world under the GDPR is a utopia and Europe is lucky enough to be still quite close to the US but it is completely different with China or other authoritarian countries.” Of course, it would be great if this was applied in China and elsewhere, but it seems very complicated from his point of view. Maybe dialogue and putting water in the wine between each country could develop a common standard. Taking the most interesting markets one by one would perhaps be good to make the weaker countries follow these standards and thus convert all the other countries.

Appendix

Figure 1

Row Labels	Average of Amount €
AUSTRIA	€ 3,009,850.00
BELGIUM	€ 6,500.00
BULGARIA	€ 199,903.75
CYPRUS	€ 15,125.00
CZECH REPUBLIC	€ 1,733.64
DENMARK	€ 180,425.00
FRANCE	€ 10,220,000.00
GERMANY	€ 1,465,572.06
GREECE	€ 122,500.00
HUNGARY	€ 13,555.79
ITALY	€ 3,850,000.00
LATVIA	€ 78,500.00
LITHUANIA	€ 61,500.00
MALTA	€ 5,000.00
NORWAY	€ 186,500.00
POLAND	€ 186,866.00
PORTUGAL	€ 106,000.00
ROMANIA	€ 23,071.43
SLOVAKIA	€ 45,000.00
SPAIN	€ 36,273.81
SWEDEN	€ 26,815.00
THE NETHERLANDS	€ 470,000.00
UNITED KINGDOM	€ 105,103,400.00
Grand Total	**€ 2,368,756.30**



Source: https://medium.com/swlh/an-empirical-analysis-of-gdprs-fines-to-date-feb-2020-and-what-it-means-for-organizations-430191d6b6e8

Bibliography:

European Commission. (2021, March 9). *Europe's Digital Decade: digital targets for 2030.* Retrieved from: https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/europes-digital-decade-digital-targets-2030_en

Bygrave, L. A. (2010). Privacy and data protection in an international perspective. *Scandinavian studies in law*, *56*(8), 165-200. Retrieved from : https://www.scandinavianlaw.se/pdf/56-8.pdf

De Hert, P., & Papakonstantinou, V. (2021). Framing big data in the council of Europe and the EU data protection law systems: Adding 'should'to 'must'via soft law to address more than only individual harms. *Computer Law & Security Review*, *40*, 105496. Retrieved from : https://www.sciencedirect.com/science/article/pii/S0267364920301011?casa_token=suqCl6T5434AAAAA:lutknj_lOh6JdIh_Q-Folll59vMctgalyInx2RO4iiELmHEyRJ3WDqyKBjiswxUKeBwWlsBOCA

BBC Poll. http://news.bbc.co.uk/1/shared/bsp/hi/pdfs/08_03_10_BBC_internet_poll.pdf

Yeung, K., & Bygrave, L. A. (2022). Demystifying the modernized European data protection regime: Cross-disciplinary insights from legal and regulatory governance scholarship. *Regulation & Governance*, *16*(1), 137-155. Retrieved from : https://onlinelibrary.wiley.com/doi/abs/10.1111/rego.12401

Ezrachi, A. (2018). EU competition law goals and the digital economy. *Oxford Legal Studies Research Paper.*

Botta, M., & Wiedemann, K. (2019). The interaction of EU competition, consumer, and data protection law in the digital economy: the regulatory dilemma in the Facebook odyssey. *The Antitrust Bulletin*, *64*(3), 428-446. Retrieved from : https://journals.sagepub.com/doi/full/10.1177/0003603X19863590

De Hert, P., & Sajfert, J. (2019). Regulating Big Data in and out of the data protection policy field: Two scenarios of post-GDPR law-making and the actor perspective. *Eur. Data Prot. L. Rev.*, *5*, 338

Wylde, V., Rawindaran, N., Lawrence, J., Balasubramanian, R., Prakash, E., Jayal, A., ... & Platts, J. (2022). Cybersecurity, Data Privacy and Blockchain: A Review. *SN Computer Science*, *3*(2), 1-12
Retrieved from : https://link.springer.com/article/10.1007/s42979-022-01020-4

Aho, B., & Duffield, R. (2020). Beyond surveillance capitalism: Privacy, regulation and big data in Europe and China. *Economy and Society*, *49*(2), 187-212. Retrieved from : https://www.tandfonline.com/doi/abs/10.1080/03085147.2019.1690275?casa_token=T8oB-UKy-5kAAAAA:N2ggOd4LEB4jt1aQM_D9de7x6FlvvBO7RX8w-nhKrVTeYzRhWC4FCfpiaX80HqBA1yd3Xes2sh1p

Manancourt, V. (2020). Meet the Dutchman who cried foul on Europe's tracking technology. *Politico*. Retrieved from: https://www.politico.eu/article/meet-the-dutchman-aleid-wolfsen-who-cried-foul-on-europe-coronavirus-covid19-tracking-technology/

Rühlig, T., & Björk, M. (2020). What to make of the Huawei debate? 5G network security and technology dependency in Europe. *UI Paper*, *1*, 2020. Retrieved from : https://www.ui.se/globalassets/ui.se-eng/publications/ui-publications/2020/ui-paper-no.-1-2020.pdf