GDPR AND ONLINE BEHAVIOURAL ADVERTISING: THE EXTENT TO WHICH ARTICLE 22 AND CONSENT REQUIREMENTS ARE SUFFICIENT IN SAFEGUARDING VOTERS' PRIVACY ON FACEBOOK

KANDEJEVA, KRISTINA
School of Law, College of Social Sciences

ABSTRACT

Technological advances have drastically changed our world, offering new possibilities for consumers and businesses but raising serious concerns about the data subject's privacy and the extent to which it can be safeguarded. This is especially concerning in the context of the use of data for political advertisements on social media platforms. This article focuses on exploring the extent to which the UK-GDPR safeguards voters' privacy in the context of online behavioural advertising on Facebook. Specifically, the consent requirement and Article 22 are the main focus. The article concludes that despite its broad scope GDPR may offer substantial safeguard; however, in the absence of case law, many of its broad concepts require clarification by courts. Finally, as the UK is free to divert from the EU law, the recommendations made by a recent task force in relation to the consent requirement and Article 22 are also discussed.

INTRODUCTION

While digital advances offer new opportunities to consumers, the benefits often come at sacrificing the extent to which consumers can keep their data private (Veliz, 2020). As Richard Serra worded it in 1973, 'if something is free, you're the product' (Weyergraf, 1980). Originally, the quote referred to television advertising; yet, with the rise of tech giants such as Facebook or Google, it has taken on a whole new meaning. Today, these tech giants are making billions in advertising revenue and there is no indication of this rate decreasing (Issac, 2021). The 2020 COVID-19 pandemic has further accelerated the growth of Facebook advertising sales and an ever-increasing number of people spending more time online (Ofcom, 2021).

Data protection forms a part of a wider privacy debate and although it is 'notoriously hard to capture' we should debate what it entails to understand the legal protections privacy should benefit from (Koops, 2017, p. 487). In the absence of a global and harmonised privacy enforcement framework, companies are obligated to comply with regional and national privacy frameworks. In 2018, the General Data Protection Regulation (GDPR) came into force, replacing the somewhat outdated Data Protection Directive. While many were delighted with the arrival of the new legal framework, often labelled as the international gold standard for privacy regulation, for most the arrival of the GDPR was marked by countless emails from long-forgotten companies asking for their consent to continue receiving marketing emails.

To date, the debate has revolved around more fragmented and sector-based approaches. However, the Brexit referendum and the 2016 US presidential election marked another turning point in the data privacy debate. It showed the world the possibilities of social media in swaying voters. Yet little research has been carried out on the adequacy of the existing legal frameworks to safeguard the privacy of voters in the UK. There is a consensus that privacy is at the heart of the democratic voting process, yet beyond providing anonymity for voters on the ballots, the relationship between privacy and data-driven electoral campaigns has been underexplored (McDonagh, 2020).

The UK-GDPR includes some notable updates, including remarkably hefty fines. However, many provisions remain relatively unchanged, when compared to its predecessor, DPD (Edwards, 2019). This legal framework was created in the era of floppy disks, Walkmans and Nokia phones: an era before smart devices. Therefore, this sparks the question: if and to what extent is the GDPR sufficient in safeguarding the voters' privacy in the context of targeted political advertising?

This article focuses on further developing an understanding of the extent to which UK GDPR is sufficient to address the challenges raised by digital political advertising on Facebook. Privacy advocates point to the consent mechanism and Article 22 of the GDPR as measures that may help safeguard the privacy of data subjects by putting them in control of whether data relating to them is being processed. Therefore, this article will focus on two specific areas: the first subsection will be dedicated to Article 22 GDPR, and the second subsection to valid consent. Although it is uncertain whether rights under Article 22 apply to profiling for political advertising, there is a good case for arguing that it should. As political campaigners increasingly make use of personalised political advertising on Facebook, questions around profound privacy issues these practices give rise to remain under-explored.

BACKGROUND

Data mining, big data and data analytics have become buzzwords which are almost impossible to escape. From industry publications to gossip columns and celebrity news, these terms seem to appear almost everywhere. Fine-tuned advertising allows marketers to target demographics with a laser focus on an unprecedented scale. This is at the heart of the offering of social media platforms, including Facebook (McDonagh, 2020). As a result, users see different advertisements, depending on their attributes and location (Pariser, 2009). What sets this type of advertising apart from advertising on traditional media is that even people with seemingly very common demographic profiles, interests, and education may end up seeing vastly different advertisements pushed by the same advertiser, to advance the same campaign goal.

This potential of social media advertising has not gone unnoticed by political powers and parties. This was most notably demonstrated by the Cambridge Analytica scandal. It was revealed that data analytics company Cambridge Analytica

had obtained data from more than 50 million Facebook profiles to develop a technique for predicting and shaping the behaviour of individual voters. This scandal was the subject of a one-of-a-kind enquiry by the UK's DCMS committee, which found that Facebook had intentionally violated UK data and privacy laws (House of Commons Digital, Culture, Media and Sport Committee, 2019). This significant data breach demonstrates significant gaps in Facebook's data management and protection practices.

Most concerns around political advertising on social media revolve around transparency behind such advertisements, accountability and the public's ability to debate the message. This is a recent development: previously, advertising on TV and in newspapers was available in public spaces, and everyone would see the same content. This is a stark contrast to Facebook advertising, which is delivered because of personal data processing (Borgesius, 2016). There are some arguments that data used in targeted advertising is nameless, as it does not contain personal identifiers such as persons' names or home addresses (Urban et al., 2020). Consequently, this lack of consensus on the mechanism delivering this type of advertising may partially explain the lack of regulation.

Nevertheless, political advertising on Facebook is especially worrying when considering that political TV advertising is banned in the UK, albeit there is a limited exception to the rule (Animal Defenders International v the United Kingdom, 2013). The rationale behind such a ban is the need to 'sustain a balance of views' (Animal Defenders International v the United Kingdom, 2013). Paradoxically, political advertising goes practically unregulated on social media; a tool that can potentially reach the same number of people at a much lower cost. In the early days of the tech boom, it was argued that 'democracy presumes and maintains the rule of law […] often defined in reference to the protection of human rights' (Hildebrandt, 2008, p.61). Therefore, for many, this practice of personal data commodification with the aim of profit-making, also known as surveillance capitalism, is 'profoundly anti-democratic' (Zuboff, 2018).

Facebook has attempted to provide mechanisms to improve transparency, most recently by launching Facebook's Ad Library; a database of every active ad on Facebook. However, a recent study has concluded that the design and implementation flaws of the tool significantly degrade the transparency it aims to provide (Edelson, 2020). Nevertheless, according to Facebook's Ad Library tool, the UK government has invested over £1m in advertising on the platform since November 2018 (Facebook Ad Library). The UK's political parties have spent an average of £500,000 since November 29th 2019, with the Conservative and Labour Parties being the biggest spenders.

Furthermore, much of the challenge in regulating this space lies in the changing landscape. Today's rapid and fluid technological growth has created a space difficult to capture and define (Krotoszynski, 2020). Naturally, the question may also arise if the data processed by Facebook in delivering the advertising solutions benefit from the protection afforded by the UK-GDPR. While the discussion of social media and democracy is too vast for the scope of this article, Zuboff points out two regulatory areas at our disposal to regulate surveillance capitalism: data protection and monopoly power regulations. The focus of this article is the former.

To capture the scale of the problem, it is important to outline just how much more powerful online behavioural adverting is in comparison to advertising on traditional media. A recent study concluded that marketers utilise an average of as many as 80 personal attributes for a campaign's targeting settings (Andreou, 2021). Targeting functions span vastly beyond traditional location, education, age or gender, instead offering detailed targeting options such as health charities a user is interested in, or money-saving pages they follow. While users unconsciously expose their health or financial information, in the hope to learn some money-saving tricks, advertisers can capitalise on it. There is also the possibility to target users who are similar to those an advertiser already has in their database. Exactly how this similarity is determined by the platform is unknown. As much about the algorithm behind Facebook's Ad Tech remains a mystery, according to Pew Research Centre in 2019, three-quarters of Facebook users are unaware of the platform's practices to track and profile them.

Consequently, this raises fears about political manipulation that may have the potential to impact Western democracies, including the UK where Cambridge Analytica sparked a debate among policymakers and privacy advocates (Fink, 2020). A three-year probe by the ICO concluded that Cambridge Analytica was not involved in the Brexit referendum 'beyond some initial enquiries made' (ICOb, 2018). Yet Dominic Cummings, a former governmental advisor, confirmed that almost all the financial resources of the campaigners were directed towards digital advertising (Hankey, 2020). Although the extent to which Cambridge Analytica may have swayed the voters one way or another is still debated, privacy advocates argue that it should not be left up to private companies and their goodwill to preserve our most basic values, including human rights and democracy (Veliz, 2020). As the use of advertising tools offered by Facebook demonstrated in the Cambridge Analytica scandal, the intent to sway the voters was there.

METHODOLOGY

This article focuses on exploring the extent to which the UK-GDPR safeguards voters' privacy in the context of online behavioural advertising on Facebook. Other types of online advertising, such as search engines or display advertising, will not be considered in this article. The reason for excluding these other types of advertising is two-fold. Firstly, social media advertising has been at the forefront of the debate around political advertising in the run-up to the Brexit Referendum. Secondly, the advertising mechanisms behind these advertising technologies are different. While search advertising requires a more active approach, i.e., a user actively 'googling' specific keywords, social media advertising is more passive; users can be exposed to advertisers without actively seeking information on relevant topics. Subsequently, the key questions to investigate are:

a) Do regulatory efforts lag behind the fast developments in advertising technology on Facebook?

b) Are the key provisions in the UK GDPR sufficient to safeguard voters from having their data weaponised by political advertisers?

To answer these questions, the article will discuss three objectives:

a) Why, for many privacy advocates, Article 22 of the UK-GDPR may provide a much-needed solution for regulating data usage for online behavioural advertising.

b) The extent to which this provision may be used to safeguard voters' privacy.

c) If the relevant consent provisions of the UK-GDPR are sufficient in safeguarding voters from having their data utilised in targeted political adverting.

Data/Sources

This is theoretical research, focused on the analysis and evaluation of the legal provisions by studying relevant

academic literature and European case law. To further enhance this discussion, it will be contrasted with industry articles and relevant audits and reports:

a) A report on Cambridge Analytica and Data Breaches by the ICO.

b) A Task Force report on the future of data protection in the UK, following Brexit.

The basis for this approach is to help the reader explore the asymmetry between technical development and regulatory efforts.

ARTICLE 22 OF THE UK GDPR

The focus of the following section is to examine the extent to which GDPR safeguards individuals from automated decision-making in the context of targeted digital advertising. Despite its wide application, fairness and transparency of data processing lie at the heart of the GDPR. Digital advertising is one of the most obvious examples of automated decision-making, that happens with no human interference, within a matter of milliseconds. Therefore, for many, Article 22 safeguards against algorithmic decisions in the context of digital advertising. Even in the pre-Facebook advertising era, Hildebrandt (2008) identified that the dangers of profiling lay in the fact that the person is unaware that such a profile is applied to them and 'may be seduced to act in ways they would not have chosen otherwise' (pp. 63), effectively weaponizing personal data.

Within the GDPR, there are no specific rules for targeted advertising or provisions addressing the concerns around weaponizing personal data to manipulate data subjects. The key differentiator between traditional political marketing campaigns (which also saw the use of electoral data) is the extent to which these practices have become opaque (ICO, 2021). While the focus of advertising has always been to sway people and build loyalty, micro-targeting allows selecting individuals using the most intimate details about their personalities, creating a personalised message to exploit their vulnerabilities (Gallo, 2020). A recent empirical study has concluded that GDPR has not negatively affected advertising technology's ability to predict consumer behaviour; there are signs that may suggest the opposite outcome has been achieved and the ability to predict consumer behaviours has increased (Guy et al., 2020).

TARGETED ADVERTISING AND AUTOMATED DECISION MAKING

Article 22(1) of the UK GDPR provides that data subjects have the right 'not to be a subject to a decision based solely on automated means which produces legal effects concerning him or her or significantly affects him or her'. Furthermore, Article 22(4) of GDPR, providing for additional safeguards for special category data, such as political opinions, and religious or philosophical beliefs, is a new addition that its predecessor DPD was lacking. However, if and the extent to which this provision does apply to targeted advertising remains debatable, as outlined in sections below.

The phrasing of 'solely' and 'means which produces legal effects concerning him or her or similarly significantly affects him or her' are the key elements in the wording of Article 22 of the UK GDPR; however, as discussed below the interpretation of these terms is unclear. As noted, paid advertisement on Facebook is one of the most notable examples of decisions based solely on automated means. However, Article 22 does not prevent decisions based solely on automated means; rather, it qualifies it for situations when it produces legal effects. What is unclear is how far the interpretation of 'legal' or 'similarly significant' effects can be stretched. Overall, the guidance provided by the Article 29 Working Party (Art. 29 WP, 2017), which is an independent European working party now formally replaced by the European Data Protection Board, appears contradictory. It states that targeting women interested in fashion will not have a legal or similarly significant effect, yet notes that on some occasions online marketing may be considered relevant under Article 22 (Art. 29 WP, 2017). This becomes especially ambiguous when considering the capabilities of the Facebook advertising algorithm.

Further lack of clarity exists in relation to decisions that do not produce a 'legal effect', yet may still similarly significantly affect the data subject. The Art. 29 WP provides guidance on automated individual decision-making and profiling for the purpose of GDPR (Regulation (EU) 2016/679). According to the guidance, decisions will similarly significantly affect the data subject, providing a relatively high legal threshold. However, a contradiction arises as Art. 29 WP provides guidance in that 'for data processing to significantly affect someone [...] the decision must have the potential to […] affect the circumstances, behaviour or choices of individuals concerned' (The Article 29 Working Party, 2017, pp. 11). Specifically, online marketing may fall under Article 22 if it uses knowledge of the vulnerabilities of the data subjects targeted. To date, no further guidance has been provided by the new advisory body: the European Data Protection Board. As Facebook's entire advertising ecosystem is built around using knowledge about data subjects and their vulnerabilities to influence their behaviour or choices, there is a very strong argument that Article 22 should apply to safeguard social media platform users from paid political advertising. This case is even stronger when considering the serious consequences of political advertising.

To illustrate the case, in the absence of any UK case law, a recent judgment handed down by the Amsterdam District Court to Ola/Uber ride-hailing platforms may be of relevance. This case may offer some initial indication of how courts in Europe have interpreted Article 22 of the GDPR. This landmark ruling obligated a big tech company to reveal techniques, including algorithms, to assign work and deduct earnings (Strauss and Venkataramakrishnan, 2021). While the Court ruled that the processes had a meaningful human intervention, it did provide that the companies must share further details of algorithmic allocation of drivers, following more specific requests of personal data and its use by these drivers.

In a more recent case, the Italian DPA fined a food delivery company 2.6 million Euros following an investigation that uncovered a range of issues, including a failure to comply with Article 22 (EDPB, 2021). It was found that the infringement occurred as the company was carrying out profiling activities of their drivers without implementing suitable safeguards. While both cases investigate employment law matters, they nevertheless outline an increasing public awareness of automated decision-making and Article 22 of GDPR as a key safeguard mechanism. Arguably, these cases also illustrate a growing trend for data subjects to rely on Article 22 to balance legitimate business interests with the rights and freedoms of data subjects.

Cambridge Analytica may be an extreme example of the use of big data in a political advertisement. Nevertheless, other companies operating on a smaller scale offer similar services today (Strauss, 2021). However, legal remedies under the existing legal framework are nothing short of complex. Prior to the GDPR coming into force, it has been established that Article 22 presents 'a right to object' to algorithmic processing, not to demand an explanation of how the processing was done (Edwards, 2019). This interpretation is also supported in the guidance provided by Art. 29 WP, providing that 'interpreting Article 22 as a prohibition rather than a right to be invoked

means that individuals are automatically protected' (Edwards, 2019). However, as demonstrated in the Uber/Ola case law, even when the algorithmic system was reviewed by a 'human eye', a court may order a further disclosure of the algorithmic system. Yet a major challenge for such an approach is the revelation of several engineers employed by the big tech companies. It has been confirmed that even experts and those who designed the algorithm may not always understand how the inputs become outputs (Waldman, 2019). This is due to computers' unique ability to find relationships between series of outputs, delivering outcomes that are unexpected and potentially would not have been discovered with a 'human eye' (Waldman, 2019). One extreme solution in the given case would be a blanket ban on political advertising on social media, like the existing ban on political TV advertising. Yet, such an approach would come with its own challenges that are beyond the scope of this article.

Another possibility is that UK lawmakers may take a significant change in their approach to automated decision-making altogether. There is an indication that this may be the case in a recent report published by the UK task force on Innovation, Growth and Regulatory Reform. This report recommends cutting the protections afforded by the GDPR, including removing Article 22 and refocusing on the legitimacy of automated decision-making (Smith, 2021). While the privacy advocates argue that despite the challenges posed by the complexity of algorithms, the outputs it produces and the potentially broad scope of the GDPR, the regulation can offer much-needed robust protection. Therefore, the recommendation by the task force to remove Article 22, due to it being 'burdensome, costly and impractical for organisations to use' (Waldman, 2019), may be heavily criticised by privacy advocates. This is worrying as the Facebook advertising algorithm has moved beyond understanding users or their interests, to knowing which user will fulfil which goal at what time. This capability to find unexpected correlations arguably makes it privacy-invasive (O'Neil, 2016), as raw unrelated data put together can reveal sensitive information, challenging democratic principles.

CONSENT REQUIREMENT

As discussed in the previous section, many privacy advocates point to Article 22, regulating automated decision-making, as a key provision for safeguarding voters' privacy in the context of targeted political advertising on social media networks. The focus of this section is the consent requirement, another area that according to privacy advocates has the capability of safeguarding users' privacy on social media, specifically Facebook. This is an area of major change when compared to its predecessor. The new regulation sets out to eliminate any grey areas that could have previously occurred (Edwards, 2019).

The GDPR provides consent as the prime legal basis for processing personal data, albeit it is not the only one and the new regulation has introduced some positive changes. The consent requirement is defined in Article 4(11), while Article 7 sets out further conditions. These provisions further reinforce the overarching goals of lawfulness, fairness, and transparency that the GDPR aims to achieve. Previously, critics argued that DPD allowed plenty of room for the interpretation of 'consent', potentially leaving the room open to harm the data subjects (Edwards, 2019).

The detailed consent provision sets out a range of conditions; the UK-GDPR provides that consent is 'freely given, specific, informed and unambiguous indication of the data subject's wishes'. This phrasing affirms the notion that in a situation where there is no choice the consent obtained isn't freely given and valid (Savin, 2020). This is a stark contrast to the pre-GDPR era, where the consent and pre-ticked boxes acted like a 'magic wand' to justify the data processing (Massey, 2018). Significantly, consent as a condition of a contract or a provision of a service and the pre-ticked boxes have been specifically outlawed by the updated regulation.

Consent is also an exception for automated decision-making based on sensitive data (such as political views), providing that data subjects may be subject to a solely automated profiling if the decision 'is based on the data subject's explicit consent' (Article 22(c) UK-GDPR). Nevertheless, there are concerns that privacy policies have become increasingly extensive and difficult for non-legal professionals to read. This calls into question the effectiveness of the new requirement set by the GDPR of a positive action taken by the data subject to consent. Subsequently, it is easy to picture circumstances in which the data subject may consent to processing of sensitive data without wholly understanding the implications of such consent. For example, a complaint against Google was brought forward to the French Data Authority CNIL. Here it was found that the conditions of a valid consent for personalised ads in accordance with the GDPR were not satisfied (CNIL, 2021).

These conditions for a valid consent are provided for in Article 7. To date, few studies have been conducted to understand the compatibility of the GDPR's consent requirements with Facebook's targeted advertising. However, there is considerable academic contribution exploring online contracts in general, with the credibility behind it, including phrases such as 'I have read and I agree', often being called the most frequent lie on the internet (Davey, 2019). A tendency toward lack of clarity and transparency when contracting online can still be observed. Nothing suggests that agreeing to the terms and conditions of social media platforms and its privacy policies is an exception. For example, as demonstrated in Figure 1 below, when creating a new Facebook account, the user automatically agrees to Facebook's Terms, Data Policy and Cookie Policy, without an option to agree to just one or two of these policies. Arguably, in this case, the consent to accept the terms and conditions of the platform, including the use of personal data for advertising purposes, is bundled together with the sign-up for the service (Geradin, Karanikioti and Katsifis, 2021).

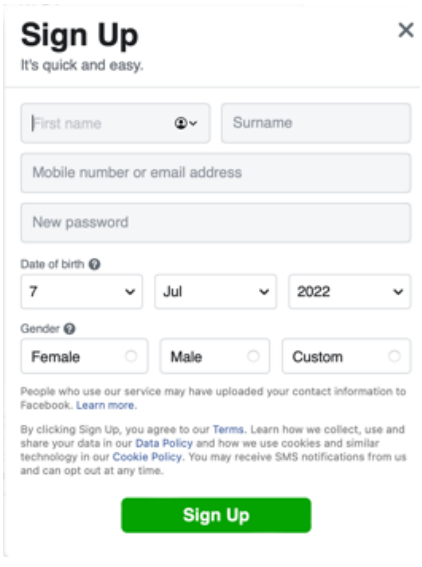

Figure 1: Facebook sign-up page. There is no option to sign up without agreeing to Facebook's advertising policies.

Some argue that consent mechanisms for social media advertising do not comply with the requirements laid out in the GDPR (Joyee De and Imine, 2020). Although Facebook states that data protection is central to its activities and the platform is fully complicit with the GDPR, this may be questioned due to its track record and most notably the Cambridge Analytica scandal. The WhatsApp takeover in 2014 is another example of the platform's poor track record in being transparent with its data management practices. On this occasion, the European Commission concluded that employees at Facebook were aware of the technical possibilities to link data between two companies, Facebook and WhatsApp, despite stating the contrary. Facebook could link users' WhatsApp phone numbers with users' Facebook profiles (European Commission, 2017).

Users are willing to accept potentially privacy-invasive technologies in exchange for services such as free messaging (Davey, 2019). The failure of the Delete Facebook movement following the Cambridge Analytica scandal illustrates this power imbalance. In essence, consent can only be valid if the user has a real choice between consenting to data processing without suffering any negative consequences if they do not consent (Geradin, Karanikioti and Katsifis, 2021). The idea of 'freely given' consent is at the heart of these provisions, giving people choice and control over how their data is used. According to GDPR Article 4(11), in assessing whether consent is freely given 'utmost account' must be taken of whether the performance of the contract is made conditional on the consent to data processing. Therefore, it can be questioned if there ever was valid consent to targeted advertising, as the user is unable to use the platform without consenting to targeted political advertising.

However, there is a clear case for arguing that valid consent requirements set out in GDPR are not satisfied in Facebook's sign-up process. There are no tick boxes and no opportunity to provide an affirmative indication that the user consents to these data management practices. Instead, a user is provided with a statement that, 'By clicking Sign Up, you agree to our Terms. Learn how we collect, use and share your data in our Data Policy', as shown in Figure 1. Facebook's Data Policy stipulates that the platform collects content and communication the user provides, including content creation, sharing, and messaging, to automatically analyse the context and provides a personalised version of Facebook's products. Arguably, the action taken by the user is rather passive and the ability to use the platform is conditional to the user accepting Facebook collecting communication and content the user provides.

The user has some remedies, such as the ability to remove an interest based on which they are targeted or the association with a specific brand: both attributes are used in targeting. However, this is only a partial remedy and arguably does not satisfy the consent requirements set out in Article 7. There is a good case for arguing that there was no valid consent to this type of advertising in the first place. Instead, having to untick yourself from a specific interest or consumer category may be likened to a pre-ticked box, which does not comply with the GDPR. Therefore, in GDPR terms this may constitute a way users can exercise their right to object, rather than consent.

To further support this analysis, similarities can be drawn between the way Facebook allows users to control the interests for which they're being targeted, to the tools provided by Google, which were found to be incompatible with the GDPR (Tambou, 2019). However, it has been reported that Facebook has allocated a budget for fines for the GDPR breaches, with it increasingly being seen as a part of its 'business cost' (CPO Magazine, 2022). In March 2022, Meta was issued with a €17m fine, following an enquiry into 12 personal data breaches (BBC, 2022), yet despite fines for data breaches achieving record levels, it is only a fraction of Facebook's and its parent company Meta's annual turnover (Satariano, 2021).

To comply with the GDPR requirements, the user's consent must also be informed. The relationship between informed consent and political views (which is provided as the special category data in the regulation) is worth investigating. While the data policy states that users' political views are afforded special protection and this information is provided by the user in their profile fields or life events, there is no mention of how this information is protected if it is an unexpected outcome of the algorithmic processing (McDonagh, 2020). Such outcomes are entirely plausible, as discussed in Part I of this paper. Therefore, it is unclear to what extent the user is protected if they have chosen not to enter their political views; however, the platform has built their political profile based on their location, education, places visited, non-political content created, and messages shared. Furthermore, the ability of marketers to utilise the knowledge of their demographics to implement a workaround to avoid the protection afforded to the special category data should also be acknowledged. Albeit should they choose to target political opinions directly, explicit consent is one of the conditions as set out by Article 9 of the GDPR. Based on Facebook's Data policy, it appears that such 'explicit' consent is granted when entering political views as a part of the profile information or updating life events.

The future of the consent requirements and the protections it provides in the UK is unclear. On one side the report published by the ICO in 2018 stipulates that one of the policy safeguards proposed in the wake of the Cambridge Analytica scandal may be a requirement of a third-party audit. This audit would aim to ensure that appropriate consent has been obtained and/or personal data obtained by the party is deleted (ICO, 2018). On the other hand, a more recent report by the Innovation, Growth Taskforce proposes to relax consent requirements to support the growth of the AI sector, replacing it with a 'legitimate interest' test (Smith, 2021). No further guidance is provided on what would constitute a 'legitimate interest' according to this task force. However, it is possible to turn to ICO for further guidance on what would constitute a 'legitimate interest' according to the UK GDPR today. It is the most flexible lawful basis for data processing, and the test can be broken into three parts: purpose test, necessity test and balancing test. Detailed guidance on all three parts of the test is available on the ICO website; it is noted that in cases of direct marketing individuals' rights are absolute and should they object to being marketed to, the advertiser must stop immediately (ICO, 2021b). Nevertheless, this is a speculative approach to 'legitimate interest' with no clear answer, as it is unclear if when implementing taskforce recommendations, this approach would not be amended.

CONCLUSION

By looking at Article 22 and the consent requirement of the UK GDPR, this article explored the extent to which the UK GDPR is sufficient in safeguarding voters' privacy in the context of targeted advertising on Facebook. This paper evaluated a fast-paced area with many developments from various stakeholders. To address this challenge, the research focuses specifically on the UK GDPR, its relevant provisions and targeted advertising on Facebook. In the absence of case law in the UK, the experience of other European countries was analysed.

First, this article concluded that the extent to which privacy advocates could rely on Article 22 to safeguard voters from targeted political advertisements on Facebook, isn't clear. On one hand, it may appear that Facebook advertising falls outside the scope of the article. On the other hand, guidance by Art. 29 WP suggests there may be scope to extend the protections afforded by the article to political advertising on Facebook.

Second, this article concluded that there is a good reason to suspect that Facebook's advertising mechanisms are not compatible with the UK-GDPR consent requirement. It could also be argued that the GDPR consent requirement supports the democratic process, as political parties wishing to target their voters would have to obtain voters' consent. However, following Brexit the UK can divert from principles set out in GDPR and further amend the UK GDPR, significantly lessening voters' protection. This article briefly looked at the future of the UK GDPR, by analysing a report by the Innovation, Growth Taskforce, it concluded that some worrying recommendations have been made, which, if and when implemented, may lessen the existing safeguards.

REFERENCES

Animal Defenders International v United Kingdom App no 48876/08 (ECtHR, 22 April 2013)

Andreou, A., Silva, M., Benevenuto, F., Goga, O., Loiiseau, P., and Mislove, A. (2019). "Measuring the Facebook Advertising Ecosystem." NDSS 2019 – *Proceedings of the Network Distribution System Security Symposium*, San Diego, United States, pp. 1-15.

Aridor, G., Che, Y-K., and Salz, T. (2020). "The Economic Consequences of Data Privacy Regulation: Empirical Evidence from GDPR." Cambridge, MA, USA: *National Bureau of Economic Research*.

Article 29 Data Protection Working Party (2018). "Guidelines on Automated individual decision-making and Profiling for the purpose of Regulation 2016/679" [online] Available at: https://ec.europa.eu/newsroom/article29/redirection/document/49826 [Accessed 7 June 2022]

BBC News (2022). "Facebook fined €17m for breaching EU data privacy laws." [online] Available at: https://www.bbc.co.uk/news/articles/cp9yenpgjwzo [Accessed 5 June 2022]

Koops, B. J., Newell, B. C., Timan, T., Skorvanek, I., Chokrevski, T., and Galic, M. (2017). "A Typology of Privacy." *University of Pennsylvania Journal of International* Law **483**, pp. 483-757.

Borgesius, Z. J. F. (2016). "Singling out people without knowing their names – Behavioural targeting, pseudonymous data, and the new Data Protection Regulation." *Computer Law & Security Review* **32**, pp. 256-71.

CNIL (2021). "The CNIL's restricted committee imposes a financial penalty of 50 Million euros against Google LLC." [online] Available at: https://www.cnil.fr/en/cnils-restricted-committee-imposes-financial-penalty-50-million-euros-against-google-llc [Accessed 17 May 2022]

Davey, F. (2019). "Making Contracts Online: Old wine in Smart Bottles?" in L. Edwards (Ed.), *Law, Policy and The Internet* (pp. 365-392). Oxford, UK: Hart.

Edelson, L., Lauinger, T., McCoy, D. (2020). "A Security Analysis of the Facebook Ad Library". *IEEE Symposium on Security and Privacy*, pp. 661-678.

Edwards, L. (2019). "Privacy and Data Protection: What is Privacy? Human Right, National Law, Global Protection" In L. Edwards (Ed.), *Law, Policy and the Internet* (pp. 51-76). Oxford, UK: Hart.

EDPB (2021). 'Riders: Italian SA says no to algorithms causing discrimination. A platform in the Glovo group fined EUR 2.6 million.' [online] Available at: https://edpb.europa.eu/news/national-news/2021/riders-italian-sa-says-no-algorithms-causing-discrimination-platform-glovo_en [Accessed 14 May 2022]

Fink, U. (2020). "Social Media in election campaigns. Free speech or danger for democracy?" In *Big Data, Political Campaigning and the Law* (pp. 99-113). London, UK: Routledge.

Galli, F. (2020). "Online Behavioural Advertising and Unfair Manipulation Between the GDPR and the UCPD." In M. Ebers & M. C. Gamito (Eds.), *Algorithmic Governance and Governance of Algorithms* (pp. 109-136) London, UK: Springer.

Geradin, D., Karanikioti, T., and Katsifis, D. (2021). "GDPR Myopia: how a well-intended regulation ended up favouring large online platforms - the case of ad tech." *European Competition Journal* **17**, pp. 47-92.

General Data Protection Regulation (GDPR) [2016] OJ L 119

Hankey, S., Naik, R., and Wright, G. (2020). "Data and political campaigning in the era of big data – the UK experience." In N. Witzleb, M. Paterson & J. Richardson (Eds.), *Big Data, Political Campaigning and the Law*. London, UK: Routledge.

House of Commons Digital, Culture, Media and Sport Committee (2019). "Disinformation and 'fake news': Final Report" [online] Available at: https://publications.parliament.uk/pa/cm201719/cmselect/cmcumeds/1791/1791.pdf [Accessed 15 June 2022]

ICO (2018). "Democracy Disrupted? Personal Information and political influence" [online] Available at: https://ico.org.uk/media/2259369/democracy-disrupted-110718.pdf [Accessed 3 June 2022]

ICO (2021). "Guide to General Data Protection Regulation (GDPR)" [online] Available at: https://ico.org.uk/media/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr-1-1.pdf [Accessed 27 May 2022]

Issac, M. (2021). "Facebook's profit surges 101 percent on strong ad sales." [online] Available at: https://www.nytimes.com/2021/07/28/business/facebook-q2-earnings.html [Accessed 28 May 2022]

Joyee, D. S., and Imine, A. (2020). "Consent for targeted advertising: the case of Facebook." *AI and Society* **35**, pp. 1055-1064.

Massey, R. (2018). “GDPR Consent - UK's ICO Guidance Re-Delivers the Message That Consent Is Not the Silver Bullet for GDPR Compliance.” Entertainment Law Review 2.

McDonagh, M. (2020). “Freedom of processing of personal data for the purpose of electoral activities after the GDPR.” In N., Witzleb, M.Paterson & J.Richardson (Eds.), *Big Data, Political Campaigning and the Law*. London, UK: Routledge.

Krotoszynski, R. (2020). “Big Data and the electoral process in the United States.” In N., Witzleb, M.Paterson & J.Richardson (Eds.), Big Data, *Political Campaigning and the Law*. London, UK: Routledge.

Strauss, D., and Venkataramakrishnan, S. (2021). “Dutch court rulings break new ground on gig worker data rights.” [online] Available at: https://www.ft.com/content/334d1ca5-26af-40c7-a9c5-c76e3e57fba1 [Accessed 19 May 2022]

Ofcom (2021). “UK’s internet use surges to record levels” [online] Available at: https://www.ofcom.org.uk/about-ofcom/latest/media/media-releases/2020/uk-internet-use-surges [Accessed 25 May 2022]

O'Neil, C. (2016) Weapons of Math Destruction London, UK: Crown Books

Pew Research Center (2019). “Facebook Algorithms and Personal Data”. [online] Available at: https://www.pewresearch.org/internet/2019/01/16/facebook-algorithms-and-personal-data/ [Accessed 5 June 2022]

‘R. (on the application of Animal Defenders International) v Secretary of State for Culture, Media and Sport’ [2008] UKHL 15;

Smith, I. D., Villiers, T., and Freeman, G. (2021) “Taskforce on Innovation, Growth and Regulatory Reform” [online] Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/994125/FINAL_TIGRR_REPORT__1_.pdf [Accessed 2 June 2022]

Savin, A. (2020). “EU Internet Law” Cheltenham: Edward Elgar Publishing

Satariano, A. (2021). “Facebook’s WhatsApp is fined for breaking the EU’s data privacy law”. Available at: https://www.nytimes.com/2021/09/02/business/facebook-whatsapp-privacy-fine.html [Accessed 1 June 2022]

Tambou, O. (2019). “Lessons from the First Post-GDPR Fines of the CNIL against Google LLC”. *The European Data Protection Law Review* **5**, pp. 80-84.

Urban, T., Tatang, D., Dageling, M., and Thorsten, H. (2020). “Measuring the Impact of the GDPR on Data Sharing in Ad Networks”. *Proceedings of the 15th ACM Asia Conference on Computer and Communications Security*, pp. 222-236.

Veliz, C. (2020). Privacy is Power: Why and How You Should Take Back Control of Your Data London UK: Bentam Press

Weyergraf, C. (1980). Richard Serra: Interview, etc. 1970-1980. *The Hudson River Museum*

Waldman, E. A. (2019). “Power, Process and Automated Decision Making.” *Fordham Law Review* 2, pp. 613-632

Zuboff, S. (2018). “The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power” London, UK: Profile Books.