Hertie School
Centre for
Digital Governance

Student working paper series

The spread of hacked materials on Twitter: A threat to democracy?

A case study of the 2017 Macron Leaks

Gaia Gibeon, MPP 2022
Hanna-Sophie Bollmann, MPP 2022

23 July 2022

#digitalgovernance

Elections are democracy's most important yet most vulnerable moment. Interference in the process presents an attack on the foundations of trust and knowledge in a democratic society, as seen in the Macron Leaks, a hack-and-leak operation spread on Twitter on the eve of the 2017 French presidential elections. Hack-and-leaks have become a popular modus operandi for foreign actors, often backed by Russia, to meddle and undermine democratic elections.
First, we discuss the challenges democracies face by hack-and-leaks, then we turn to explore Twitter's past attempts to self-regulate hacked materials. These were made in response to political events in the US and changing public pressure in the US, putting the platform at risk of becoming a plaything of populist movements and foreign actors seeking to undermine democracy. Until recently, the EU lacked any adequate response but the recently published revised version of the EU's Code of Practice on Dis-information (June 2022) may signal a change. Twitter has signed the Code and promises to adopt and implement policies to prevent the spread of manipulative behaviour. Should Twitter change its Hacked Materials Policy, it will be the first time it is done in response to regulatory measures.

Note of Transparency: the authors were in touch via email with Dr. Julian Jaursch (Stiftung Neue Verantwortung) and Dr. Jörg Pohle (Alexander von Humboldt Institute for Internet and Society) to ask for advice in the research for potential EU regulation of hacked materials distribution on social media. Dr. Julian Jaursch provided the idea to check the guidelines for the new EU Code on Dis-information and Dr. Jörg Pohle provided information on the GDPR "legitimate interest test", mentioned in chapter seven.

Table of Contents

1 Introduction

"Il en va de notre démocratie, il en va de notre souveraineté, il en va de notre indépendance nationale" (Untersinger, 2017) said then French Minister of Foreign Affairs, Jean-Marc Ayrault, about the Kremlin-orchestrated hack of the Macron campaign in 2017. Essentially: this is a threat to our democracy, sovereignty, and national independence. The so-called Macron Leaks present one of the most prominent cases of hacked materials being spread via social media, which given their timing, were likely an attempt of election interference. French newspapers, like *Le Monde*, refer to the journalistic code of ethics in their reasoning for not reporting on the content of the hacked materials. The 15 gigabytes (GB) of material were simply too much to be checked for their authenticity and responsibly reported on under the media blackout regulations. French election law does not permit traditional media to report on the candidates in the 24 hours leading up to the election day (Le Monde, 2017). On Twitter, on the other hand, the materials were spread widely – the journalistic code of ethics and election laws regulating traditional news media seemed not to apply here. How to deal with hacked materials on Twitter, accordingly, presents a challenge to democracy and the platform has responded by publishing a self-regulatory "Distribution of Hacked Materials Policy".

This case study will respond to the two-part research question: What was Twitter's motivation behind its self-regulation of the distribution of hacked materials, and is it an adequate response to this challenge to democracy?

To respond to this question, we first introduce the case of the Macron Leaks. Secondly, we define the different layers of challenges to democracy presented by the case. Next, we introduce the typology of self-regulation developed by Price & Verhulst (2000) which will then be applied to Twitter's Hacked Materials Policy to answer the first part of our research question. In our conclusion, we will assess whether the policy is an adequate response to the issue of hacked materials distribution via social media and discuss the advantages and disadvantages of the approach.

2 The case of the Macron Leaks

French presidential elections have two rounds. In 2017's second round, the two leading nominees, Emmanuel Macron and Marine Le Pen, faced each other in a runoff on Sunday, 7 May. In the night between Friday and Saturday, an information leak was published, dubbed the EMLEAKS and the Macron Leaks. The 15GB of material had been obtained through hacks on the Macron campaign. A link to the hacked materials was first posted via

PasteBin on 4chan, an American discussion board. Next, they were circulated on Twitter by alt-right American activists, known for promoting conspiracy theories, and were later shared by the Wikileaks Twitter account, where the materials gained international attention and started to spread quickly (Pierron, 2017).

The leak and distribution of the materials coincided with the start of the election silence, or media blackout. This is mandated by the French Election Code, which prohibits the broadcasting of "any message having the character of electoral propaganda" starting midnight on the eve of an election, meaning between Friday and Saturday in 2017 (Conseil Constitutionnel Présidentielle, 2017a).

The media had a window to report on the publication of the leak, but had no time to review, verify and responsibly report on the contents due to the blackout deadline and the 15GB of decompressed data (Almasy, 2017; Vilmer, 2019). The Macron campaign released a statement connecting the leak to hacking efforts made against the campaign, verifying some of the documents as legitimate while stressing others were forged. The statement also included criticism on the timing of the publication, claiming it as part of an effort of democratic destabilisation as was seen in the US presidential election the year before (Pierron, 2017). The timing of the leak was a "direct attempt to manipulate the electoral process through the vulnerability created by the electoral silence period" (Downing & Ahmed, 2019, p.260).

The French Election Committee released a statement on the Saturday morning that it was notified by the Macron campaign of the leak which also contains forged documents, and reminded the media "of the responsibilities they must bear, when the free expression of the voters and the sincerity of the vote is at stake" and "asks press bodies, and in particular their websites, not to report on the content of this data" (CNCCEP, 2017).

Around January and February 2017, when Macron gained a lead in the polls, targeted manipulated-information campaigns against him became more aggressive by two main sources: the Kremlin media and American alt-right (Vilmer, 2019). In addition, the Macron campaign revealed they were the target of several cyber-attacks throughout the election period, some of which could be attributed to Russia and had been successful (Willsher & Henley, 2017). While the French government never officially attributed the hack nor the leak to Russian-backed actors, analysis by researchers and cyber security companies claim the evidence shows Russian interests in undermining the French elections. There were Russian-like patterns in the hack, evidence that was also supported by the US National Security Agency (Baines & Jones, 2018), and significant involvement and influence of the

American alt-right in the manipulative discourse on the leak (Downing & Ahmed, 2019; Vilmer, 2019).

Despite being leaked and distributed via Twitter, researchers agree that the attempt to influence the elections failed and offer several explanations (Ferrara, 2017; Vilmer, 2019). Analysing tweets related to the French election, Ferrara found the baseline general *discussion* on the elections involved "systematically and significantly more French users (thus, likely French voters), which exhibited a clear trend in favour of supporting now-president Emmanuel Macron", while the *audience* in the discussion on the Macron Leaks involved mostly English-speakers and the alt-right American community (2017, p. 15). In addition, the highly regulated media environment during the election period in France made it less vulnerable to election meddling, with regulation forbidding paid political advertisement and mandating the media blackout (Vilmer, 2019). The French also have strong traditions in the quality of journalism, of which 75% of the population trusts, compared to only 25% who trust news from social media (Vilmer, 2019).

3 Leaking and distributing hacked materials via social media as a challenge for democracy

The Macron Leaks manifest the leaking and distributing of hacked materials on social media as a challenge for democracy at two levels. First is the general challenge of a lack of code of ethics for publications and distribution mechanisms on social media platforms. Second, for the specific Macron Leaks case, is the journalistic vacuum created by election silence periods resulting in social media platforms holding disproportionate control over the political discourse in this period of time. Both challenges (even more so in combination) have the potential to undermine elections in several liberal democracies. The imperative need to regulate the leaking and distributing of hacked materials on social media becomes apparent when looking at both challenges in detail, which shall be done in the following section.

The overarching challenge behind hacked materials and social media stems from the fact that social media platforms share some decisive features with media companies – but are governed and regulated as technology companies. As pointed out by Stockmann (2020), there a several aspects setting social media platforms apart from traditional media companies, such as ownership structures and business models. However, Manovich (2009) argues that many users consume content on social media platforms

like they would consume traditional media and only rarely post themselves. In support of this argument, studies such as the Reuters Institute Digital News Report have found that individuals around the globe are increasingly getting their news through social media instead of consuming traditional news media (Newman et al., 2020). Therefore, social media platforms are fulfilling the function of traditional media for many users – but are not guided by comparable journalistic standards. This can present a challenge to democracy in many areas; the distribution of hacked and leaked materials being one of them. Journalistic code of ethics demand that hacked materials be checked for their authenticity and that privacy be carefully weighed against public interest. Social media platforms and their users do not subscribe to such a code of ethics which is why hacked materials can be leaked and distributed, often mixed with dis-information. This can be particularly dangerous in societies without solid traditional news media or low trust in traditional news media.

As seen in the case of the Macron Leaks, the French population's high level of trust in traditional news media was one of the reasons why the leak was not able to impact the election. On the other hand, the high level of accountability in French journalism paradoxically contributed to a particular vulnerability of the French democracy in the case of the Macron Leaks. Their compliance with the election silence produced a journalistic vacuum:

According to the French Constitutional Council's dedicated website for the 2017 elections, the restrictions on communication, including on the internet, during the blackout time "are intended to guarantee the freedom of expression of voters and to prevent any pressure likely to alter the sincerity of the election." [translation by Google Translate] (Conseil Constitutionnel Présidentielle, 2017b).

Several European democracies have their own version of blackout periods before elections. Up until the Macron Leaks, they rarely received any attention or were brought into question. However, the case shows that the democratic institutions of freedom of speech and free press are not the only ones that were being maliciously used: the election silence period had been turned into a vulnerability by foreign actors wishing to meddle in the election through the distribution of fake or real information at a time when it would not receive any comment from regulated and reliable media or political figures (Downing & Ahmed, 2019).

"The most influential actors were those who were most likely to pose a threat not only to the Macron campaign, but to the established rules of the election blackout. [...] we can see that it is not just the fact that a leak occurs, or indeed the content of the leaks that are important for democracy,

but also who spreads the narratives during election blackouts." (Downing & Ahmed, 2019, p.268)

In light of the media blackout, curious citizens turned to find out information on the Macron Leaks online and ultimately to Twitter, as Downing & Ahmed (2019) show in their research, using Google Trends analysis for both Macron Leaks and Twitter as search queries. It was Twitter's easy access characteristics – openness (no need for login to see tweets), indexed by Google and searchable, that made it a primary source of information (Downing & Ahmed, 2019).

In the case of France, the challenge of the distribution of hacked and leaked materials via social media was countered by a number of structural factors, such as high trust in traditional media and lack of trust in social media (Conley & Jeangène Vilmer, 2018). This failed attempt at exploiting the lack of code of ethics or an election silence period should, however, be a warning shot for other democracies whose foundations could be threatened by ineffective policies or non-regulation of hacked materials by social media platforms.

4 Timeline and context of Twitter's Hacked Materials Policy

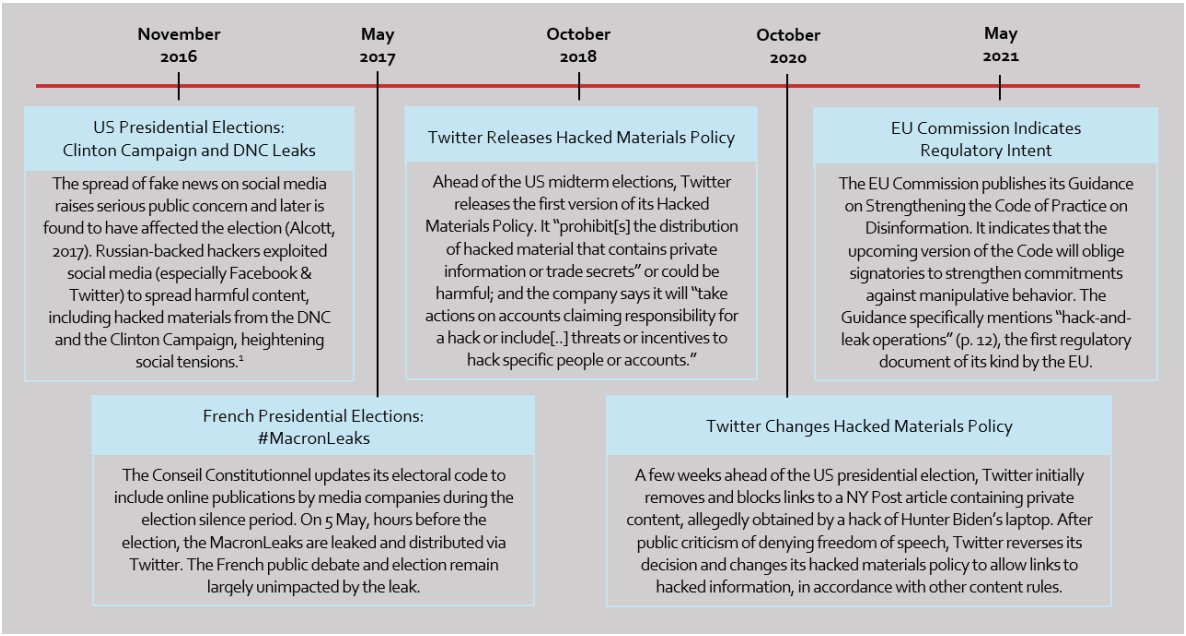

Figure 1. Timeline of changes to Twitter's Hacked Materials Policy in the context of hack-and-leak operations in the US and French elections.

Twitter has recognised the challenge the leaking and distributing of hacked materials on its platform poses to democracy, particularly to democratic processes like elections. Ahead of the US midterm elections in October 2018, it published its first self-regulation regarding the issue. Likely in response to the scrutiny the company faced after the Clinton Campaign and DNC leaks in 2016[1] (see timeline above), Twitter took a rather strict stance, announcing that its rules now "prohibit the distribution of hacked material that contains private information or trade secrets, or could put people in harm's way" (Twitter, 2018). From the side of governments, such as the US or EU, no regulation on the distribution of hacked materials was put in place after the DNC and the Macron Leaks.

Two years later, a few weeks before the US 2020 presidential elections, Twitter changed its Hacked Materials Policy, following public outcry over its blocking of Tweets on a *New York Post* article, which were suspected to contain materials obtained through a hack of Hunter Biden's laptop. Essentially, the platform decided to overhaul its former policy completely and no longer delete tweets distributing or leaking hacked materials – unless they are posted by the hackers themselves (Twitter, 2020). Vijaya Gadde, head of Legal, Policy, and Trust at Twitter, explains the change in the policy in a Twitter thread:

[1] Russian-backed hackers exploited social media (especially Facebook & Twitter) to spread harmful content, including hacked materials from the DNC and the Clinton Campaign (Greenberg, 2020); (Mueller, 2019), heightening social tensions (Bazelon, 2020).

Figure 2. Screenshots of Vijaya Gadde Tweets announcing and explaining Twitter's decision to overhaul their Hacked Materials Policy – and to allow the distribution of hacked materials, overhauling the company's previous policy.

Gadde emphasises that Twitter tried to find a balance between people's privacy and the right of free expression with the previous policy. The new policy can be understood to prioritise free expression by essentially un-regulating the leaking and distributing of hacked materials on Twitter

again. US and EU governments continued to not specifically mention or regulate the issue. Accordingly, the self-regulation typology by Price and Verhulst (2000) shall help to clarify the motivation behind Twitter's changing policies.

5 The self-regulation typology by Price and Verhulst

Communications and governance researchers Monroe Price and Stefaan Verhulst have applied broader political science theories of self-regulation (from areas such as environmental standards or engineering) to the internet in their book *The Concept of Self-Regulation and the Internet* (Price & Verhulst, 2000). Although published in 2000, many of their concepts are surprisingly applicable to the debate around social media platform regulation today. Even more so, their clear distinctions and typologies could help to structure today's less organised (due to more rapid and complex technological advancements) debates.

Price and Verhulst introduce a typology of four types of self-regulation (see table below). They differ in their relationship to government and thus in the drivers demanding the self-regulation.

	Mandated Self-Regulation	Sanctioned Self-Regulation	Coerced Self-Regulation	Voluntary Self-Regulation
Government:	... formulates framework on basis of which industry should self-regulate	... approves / disapproves of self-regulation industry has developed	... threatens to enforce binding regulation if industry does not self-regulate	...has no formal relationship to the self-regulation

Figure 3. Price and Verhulst's typology of four types of self-regulation by relationship to the governments.

Generally, the authors say that self-regulation "hardly ever exists without some relationship to the state; a relationship that itself varies greatly" (Price & Verhulst, 2000, p. 3). Furthermore, with self-regulation there is always a perceived need by the industry to regulate an issue. The source of this need can either be "the threat of public regulation, [...] a societal demand for increased responsibility by the private sector or economic factors" (Price & Verhulst, 2000, p. 4).

For the first two types of self-regulation, mandated and sanctioned self-regulation, this perceived need is the government's instruction. In both cases the government either formulates a framework on whose basis self-

regulation should be implemented (e.g., the EU Code on Disinformation) or asks the industry to come up with a framework which it will then approve or disapprove.

The third type – coerced self-regulation – is characterised by the strongest need to self-regulate effectively. The need either comes from government threatening to enforce binding regulation or from public outcry over a recent scandal which strongly demands action by the industry. Finally, in the case of voluntary self-regulation, there is no formal relationship with the government and mostly economic considerations act as the main drivers (Price & Verhulst, 2000).

6 Analysis: Why and how did Twitter self-regulate

Twitter's self-regulatory policy was the first regulatory response specifically to the challenge of the leaking and distributing of hacked materials via social media. There is no public information of a formal request by a government to regulate the issue. Nevertheless, the policy cannot be clearly assigned to any of the four types of self-regulations by Price and Verhulst. Much rather, Twitter's regulatory action seems to rest on several drivers.

Strikingly, Twitter's self-regulation of the issue, so far, is motivated mainly by US government mandates and US public debate. The Macron Leaks are likely to have played a supportive role in the first, strict removal policy. However, Twitter seems to be clearly more responsive to debates in the US which could also be due to the Macron Leaks being a failed attempt at election meddling.

Twitter's acting general counsel Sean Edgett had to testify in front of the US Congress at the end of 2017 to explain his platform's role in the election meddling practiced by Russia. While not formulating specific demands about the distribution and leaking of hacked materials, the congress requested Twitter to take action to limit the opportunities for foreign election interference operations. To many of these requests, Edgett responded with a simple "Yes, sure," unlike his counterparts from Google and Facebook who were more hesitant to agree to taking certain actions (McCarthy, 2017). When looking at Twitter's first Hacked Materials Policy which was published along with its "Update on our elections integrity work" (Twitter, 2018), one can assume that the self-regulation was a response to the US Government's mandated self-regulation formulated in the US congressional hearing. At the same time, Twitter clearly felt a strong need

to regulate, given that they enforced such a harsh policy of deleting almost all posts distributing hacked materials. This strong need likely resulted from high public pressure with users around the world outraged by the role social media platforms played in the election meddling by Russia. Accordingly, one could argue that Twitter felt coerced by the public discourse to self-regulate in a way which prioritises privacy over absolute and potentially harmful freedom of expression.

Twitter has shown to be very responsive to public debates about its practices in general. The change to its Hacked Materials Policy in 2020 can be attributed clearly to public outcry over perceived "censorship" practiced by Twitter in the deleting of Tweets sharing the NY Post article with information on Hunter Biden (Paul, 2020). The Twitter thread by Vijaya Gadde is a testament to this. Accordingly, the change in Twitter's self-regulation of the distribution of hacked materials was likely a combination of the drivers behind coerced and voluntary self-regulation. The public pressure coerced Twitter to update its policies while there likely was also an economic consideration behind this, with the comparatively small platform worried about losing users. Given that there is no public record of a political mandate to change the policy[2] and the abrupt timing of the change in the policy, one can assume that there was no government involvement behind it.

7 Conclusion: Advantages and disadvantages of the regulatory approach

Twitter self-regulated the distribution and leaking of hacked materials in two policies, in 2018 and 2020. Looking at the timeline, the first policy was a response to its laissez-faire behaviour with regards to the DNC and Macron Leaks which in one case did and in the other had the potential to undermine elections. Pressure from the public and the US Congress led to a strict blocking regulation of hacked materials which was quite effectively enforced, as demonstrated by the deleting of tweets on the Hunter Biden hack. The second policy, on the other hand, was an abrupt response solely to the public outcry about what was perceived as "censorship" particularly by Republican politicians and voters in the US. Twitter, again, responded to the political sentiment of the moment and reversed its policy completely to again adopt a laissez-faire approach to the distribution of hacked materials.

[2] Several members of the Republican party have criticized, contacted and questioned Twitter over its behaviour with regards to the Hunter Biden leaks. All these government actions happened after Twitter had already changed its policies, however (Caralle, 2020).

In the second case, there was no government involvement pushing the self-regulation.

The self-regulation approach for meeting the challenge which hacked materials pose to democracy, especially during election periods, has several advantages. First and foremost, it is a much faster response to the issue than co-regulation. Furthermore, given that the regulation of the distribution of hacked materials falls into the issue area of content moderation, self-regulation ensures minimised government intrusion in the freedom of speech field (Price & Verhulst). Given that the distribution of hacked materials is a global issue, self-regulation can be seen as a more effective response than co-regulation by one government, too. Lastly, self-regulation is more flexible in responding to changing needs.

The last point, however, precisely pinpoints the issue with self-regulation of hacked materials on social media. The two policies by Twitter showed that the company responds to current perceived political sentiments rather than developing a policy on hacked materials which would mirror the code of ethics which traditional media apply to the issue. The danger here is that Twitter does not practice a neutral stance on all hacked materials but much rather differentiates between what the public currently perceives as "good hacked materials" or "bad hacked materials". The platform risks becoming a plaything of populist movements with this approach. Furthermore, its greater responsiveness to discourse in the US compared to other countries is not an adequate response to a global challenge.

The EU Commission seems to have acknowledged the need to regulate the issue. The Guidance on Strengthening the Code of Practice on Disinformation published in 2021 is the first regulation-associated document which specifically mentions the challenge of hack-and-leak operations (European Commission, 2021). On 16 June 2022, the EU Commission published a revised version of the Code of Practice on Disinformation, listing hack-and-leak operations on the list of "impermissible manipulative behaviour" in Commitment 14 (European Commission, 2022a, p.22). Under Measure 14.1 of the code, "Relevant Signatories will adopt, reinforce and implement clear policies regarding impermissible manipulative behaviours and practices on their services".

It should be noted that the Code is not an obligatory regulation. It is the result of the work done by a variety of actors, including online platforms. The signatories decide themselves the commitments they sign up for, and it is their responsibility to ensure their policies are effective according to their commitments. The Code has been formally recognized as fulfilling the Commission's expectations (European Commission, 2022b).

Referring to hack-and-leak operations as "impermissible manipulative behaviour" makes is clear the EU Commission does not see the laissez-faire approach from the 2020 self-regulation policy as an appropriate response to the challenge of hacked materials. Twitter has committed to Commitment 14 and to Measure 14.1 specifically (Subscription Document for Twitter, 2022). In the near future, we will see what changes Twitter will make to its Hacked Materials Policy. These changes, if and when they occur, may be the first time the Hacked Materials Policy changes in response to regulatory measures, and not as a response to US political events.

In an exemplary regulatory mapping (as seen in the graph below) the current 2020 Twitter Policy is located on the extreme end of prioritizing freedom of expression. To fulfil its commitment to Measure 14.1, Twitter will need to adopt a new policy approach which prioritises disinformation regulation.

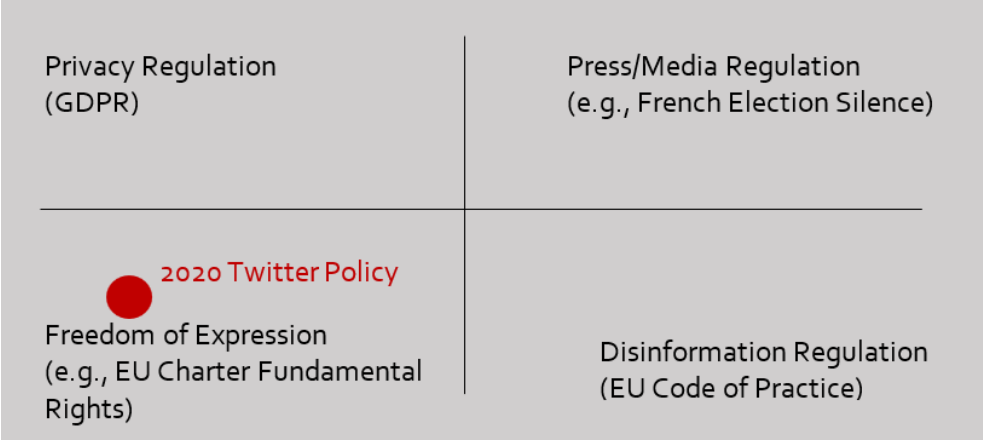

Figure 4. An exemplary regulatory mapping of the issue areas affected by hacked materials, with Twitter's 2020 Hacked Materials Policy located on the extreme end of prioritizing freedom of expression.

A more appropriate regulation would find a balance between freedom of expression and privacy. The GDPR's Article 6 Paragraph 1 Letter f could be interesting here since it demands a legitimate interest test before private data can be shared. Furthermore, particularly for the challenge of the distribution of hacked materials before elections, countries with election silence periods should adjust their electoral codes to include social media platforms. The rationale behind this logic is the argument by Manovich (2009) that there is the risk of disproportionate attention for the social media discourse caused by the journalistic vacuum.

Considering the ongoing acquisition of Twitter by Elon Musk and his announcements to limit content moderation to an absolute minimum, one could argue that co-regulation of the issue might become necessary. As

long as algorithms of social media prioritise emotionally divisive content (due to this being profitable under the current behaviourally targeted advertising business model), acting against the spread of hacked materials will not be in the interest of platforms. Given that hacked materials often contain dis-information or mal-information, this is an enormous challenge for democracy. The Macron Leaks were a warning shot for democracies around the world. With Russia's election interference activities becoming persistent (O'Connor et al., 2020), democratic governments and the EU should be on the lookout to ensure the effectiveness of hacked materials policies and consider enacting effective enforcement measures.

References

Almasy, S. (2017, May 6). Emmanuel Macron's French presidential campaign hacked. *CNN*. https://www.cnn.com/2017/05/05/europe/france-election-macron-hack-allegation/index.html. [Last Access: 14 May 2022]

Baines, P., & Jones, N. (2018). Influence and Interference in Foreign Elections. *The RUSI Journal*, 163(1), 12–19. https://doi.org/10.1080/03071847.2018.1446723.

Bazelon, E. (2020, October 13). The Problem of Free Speech in an Age of Disinformation. The New York Times. https://www.nytimes.com/2020/10/13/magazine/free-speech.html. [Last Access: 13 March 2022]

Caralle, K. (2020). 'Who the hell elected YOU?' Ted Cruz tears into Twitter's Jack Dorsey for STILL censoring tweets about Hunter Biden's emails as Republicans slam him, Facebook and Google for 'bias' - and he admits 'conservatives have lost trust in us' *Daily Mail Online*. https://www.dailymail.co.uk/news/article-8888985/GOP-senators-slam-Facebook-Twitter-censorship-suppression-conservative-voices.html. [Last Access: 28 May 2022]

Commission Nationale de Contrôle de la Campagne électorale en vue de l'élection Présidentielle (CNCCEP). (2017, May 6). *RECOMMANDATION AUX MÉDIAS SUITE À L'ATTAQUE INFORMATIQUE DONT A ÉTÉ VICTIME L'ÉQUIPE DE CAMPAGNE DE M. MACRON.* Commission Nationale de Contrôle de La Campagne Électorale En Vue de l'Élection Présidentielle. https://web.archive.org/web/20210925175533/http://www.cnccep.fr/communiques/cp14.html. [Last Access: 15 May 2022]

Conley, H. A., & Jeangène Vilmer, J.-B. (2018). Successfully Countering Russian Electoral Interference. Center for Strategic and International Studies. https://www.csis.org/analysis/successfully-countering-russian-electoral-interference. [Last Access: 28 May 2022]

Conseil Constitutionnel. (2017a). *Campagne électorale: Partie législative en vigueur*. Conseil Constitutionnel. https://presidentielle2017.conseil-constitutionnel.fr/tout-savoir/en-resume/textes-de-reference/dispositions-code-electoral-rendues-applicables/campagne-electorale-partie-legislative-vigueur. [Last Access: 15 May 2022]

Conseil Constitutionnel. (2017b*). Peut-on faire campagne sur Internet le jour et la veille du scrutin?*. Conseil Constitutionnel. https://presidentielle2017.conseil-constitutionnel.fr/tout-savoir/la-campagne-sur-internet/on-faire-campagne-internet-jour-veille-scrutin. [Last Access: 15 May 2022]

Downing, J., & Ahmed, W. (2019). #MacronLeaks as a "warning shot" for European democracies: Challenges to election blackouts presented by social media and

election meddling during the 2017 French presidential election. *French Politics*, 17(3), 257–278. https://doi.org/10.1057/s41253-019-00090-w.

European Commission. (2021). European Commission Guidance on Strengthening the Code of Practice on Disinformation. https://ec.europa.eu/digital-single-market/en/code-practice-disinformation. [Last access: 28 May 2022]

European Commission. (2022a). 2022 Strengthened Code of Practice on Disinformation. https://digital-strategy.ec.europa.eu/en/library/2022-strengthened-code-practice-disinformation. [Last Access: 20 June 2022]

European Commission. (2022b). The 2022 Code of Practice on Disinformation. https://digital-strategy.ec.europa.eu/en/policies/code-practice-disinformation. [Last Access: 20 June 2022]

Ferrara, E. (2017). Disinformation and Social Bot Operations in the Run Up to the 2017 French Presidential Election. *First Monday*, 22(8). https://doi.org/10.48550/ARXIV.1707.00086.

Greenberg, A. (2020, June 22). Hack Brief: Anonymous Stole and Leaked a Megatrove of Police Documents. *Wired*. https://www.wired.com/story/blueleaks-anonymous-law-enforcement-hack. [Last Access: 13 March 2022]

Harvery, D. & Yoel, R. (2018, October 1). An update on our elections integrity work. *Twitter.*https://blog.twitter.com/en_us/topics/company/2018/an-update-on-our-elections-integrity-work. [Last Access: 28 May 2022]

Le Monde. (2017, May 6). En marche! dénonce un piratage « massif et coordonné » de la campagne de Macron. *Le Monde*. https://www.lemonde.fr/election-presidentielle-2017/article/2017/05/06/l-equipe-d-en-marche-fait-etat-d-une-action-de-piratage-massive-et-coordonnee_5123310_4854003.html. [Last Access: 28 May 2022]

Manovich, L. (2009). The practice of everyday (media) life: From mass consumption to mass cultural production? *Critical Inquiry*, 35(2), 319–331. https://doi.org/10.1086/596645.

McCarthy, T. (2017). Facebook, Google and Twitter grilled by Congress over Russian meddling – as it happened. *The Guardian*. https://www.theguardian.com/technology/live/2017/oct/31/facebook-google-twitter-congress-russian-election-meddling-live?filterKeyEvents=false&page=with:block-59f8e5a5e4546a06df012051#block-59f8e5a5e4546a06df012051. [Last Access: 28 May 2022]

Mueller, R. S. (2019). Report on the Investigation into Russian Interference in the 2016 Presidential Election. U.S Department of Justice. https://www.justice.gov/archives/sco/file/1373816/download.

Newman, N., Fletcher, R., Schulz, A., Simge, A., & Nielsen, R. K. (2020). Reuters Institute Digital News Report 2020. Reuters Institute for the Study of Journalism. https://reutersinstitute.politics.ox.ac.uk/sites/default/files/2020-06/DNR_2020_FINAL.pdf.

O'Connor, S., Hanson, F., Currey, E., & Beattie, T. (2020). Cyber-enabled foreign interference in elections and referendums . Australian Strategic Policy Institute. https://www.aspi.org.au/report/cyber-enabled-foreign-interference-elections-and-referendums.

Paul, K. (2020, October 15). Facebook and Twitter restrict controversial New York Post story on Joe Biden. *The Guardian.* https://www.theguardian.com/technology/2020/oct/14/facebook-twitter-new-york-post-hunter-biden. [Last Access: 28 May 2022]

Pierron, M. (2017, May 5). MacronLeaks: En Marche! piraté, dénonce une "opération de déstabilisation." *LExpress.fr*. https://www.lexpress.fr/actualite/politique/elections/macronleaks-des-milliers-d-emails-de-l-equipe-de-campagne-de-macron-pirates_1905721.html. [Last Access: 14 May 2022]

Price, M. E., & Verhulst, S. (2000). The concept of self-regulation and the internet. In J. Waltermann & M. Machill (Eds.), Protecting our children on the internet: Towards a new culture of responsibility (pp. 133-198). Bertelsmann Foundation Publishers. Retrieved from http://repository.upenn.edu/asc_papers/142

Stockmann, D. (2020). Media or Corporations? Social Media Governance Between Public and Commercial Rationales. In *Advances in Corporate Governance: Comparative Perspectives, 249–268. Oxford University Press.* https://doi.org/10.1093/oso/9780198866367.003.0011.

Twitter. (2020). Twitter's policy on the distribution of hacked materials. https://help.twitter.com/en/rules-and-policies/hacked-materials. [Last Access: 28 May 2022]

Untersinger, P. M. (2017). «MacronLeaks»: ouverture d'une enquête judiciaire en France. *Le Monde*. https://www.lemonde.fr/pixels/article/2017/05/06/macronleaks-debut-d-un-long-et-fastidieux-travail-d-enquete_5123577_4408996.html. [Last Access: 28 May 2022]

Vilmer, J.-B. J. (2019). The "Macron Leaks" Operation: A Post-Mortem. Atlantic Council and the Institute for Strategic Research (IRSEM). https://www.atlanticcouncil.org/wp-content/uploads/2019/06/The_Macron_Leaks_Operation-A_Post-Mortem.pdf. [Last Access: 15 May 2022]

White, K. (2022, June 14). EU Code of Practice on Disinformation Subscription Document for Twitter. https://ec.europa.eu/newsroom/dae/redirection/document/87566. [Last Access: 20 June 2022]

Willsher, K., & Henley, J. (2017, May 6). Emmanuel Macron's campaign hacked on eve of French election. *The Guardian*. https://www.theguardian.com/world/2017/may/06/emmanuel-macron-targeted-by-hackers-on-eve-of-french-election. [Last Access: 30 March 2022]

Hertie School
Centre for
Digital Governance

Alexanderstraße 03
D – 10117 Berlin
Tel.: +49 (0)30 259219-0

Online: hertie-school.org/centre-for-digital-governance/
E-Mail: info@hertie-school.org
Twitter: @thehertieschool