dirittifondamentali.it

La CEDU su interferenze russe nei processi democratici britannici: adeguata la tutela del diritto a libere elezioni
(CEDU, sez. IV, sent. 22 luglio 2025, ric. n. 15653/22)

La Corte Edu si pronuncia sul caso riguardante la reazione del governo britannico alle segnalazioni di interferenza russa nei processi democratici del Regno Unito (ivi comprese le elezioni del 2019).
I ricorrenti hanno sostenuto che, a fronte di accuse credibili circa i tentativi della Russia di interferire nelle elezioni democratiche del Regno Unito, anche attraverso disinformazione e campagne di influenza, il Governo era venuto meno al suo dovere (un 'obbligo positivo') di indagare su tali accuse e di istituire un efficace quadro giuridico e istituzionale contro il rischio di tale interferenza.
I Giudici di Strasburgo ritengono che gli Stati non debbano rimanere passivi di fronte a prove di minacce ai propri processi democratici, conservando tuttavia ampia discrezionalità nella scelta dei mezzi per contrastarle. A giudizio della Corte, al netto di una iniziale non adeguata risposta del Regno Unito alle segnalazioni di ingerenza russa nelle elezioni interne, sono state comunque condotte due indagini approfondite e indipendenti e da allora il Governo ha adottato una serie di misure legislative e operative per contrastare le campagne di disinformazione e proteggere l'integrità democratica del Regno Unito.
Eventuali carenze, pertanto, non sono state sufficientemente gravi da compromettere la sostanza stessa del diritto dei ricorrenti, ai sensi dell'articolo 3 del Protocollo n. 1, di beneficiare di elezioni tenute 'in condizioni che garantiscano la libera espressione dell'opinione del popolo".

***

EUROPEAN COURT OF HUMAN RIGHTS
COUR EUROPÉENNE DES DROITS DE L'HOMME

FOURTH SECTION
CASE OF XXXXX AND OTHERS v. THE UNITED KINGDOM
(Application no. 15653/22)

JUDGMENT
STRASBOURG
22 July 2025

This judgment will become final in the circumstances set out in Article 44 § 2 of the Convention. It may be subject to editorial revision.

In the case of XXXXX and Others v. the United Kingdom,

The European Court of Human Rights (Fourth Section), sitting as a Chamber composed of:

Lado Chanturia, *President*,
Jolien Schukking,
Faris Vehabović,
Tim Eicke,
Lorraine Schembri Orland,
Anne Louise Bormann,
András Jakab, *judges*,
and Simeon Petrovski, *Deputy Section Registrar*,

Having regard to:

the application (no. 15653/22) against the United Kingdom of Great Britain and Northern Ireland lodged with the Court under Article 34 of the Convention for the Protection of Human Rights and Fundamental Freedoms ("the Convention") by three British nationals, Mr Ben Bradshaw, Ms Caroline Lucas and Mr Alyn Smith ("the applicants"), on 22 March 2022;

the decision to give notice to the United Kingdom Government ("the Government") of the complaints concerning Article 3 of Protocol No. 1 and to declare inadmissible identical complaints made by two additional applicants;

the observations submitted by the respondent Government and the observations in reply submitted by the applicants;

the comments submitted by the European Information Society Institute, o.z., which was granted leave to intervene by the President of the Section;

Having deliberated in private on 6 May and 24 June 2025,

Delivers the following judgment, which was adopted on that last-mentioned date:

INTRODUCTION

1. According to the applicants, Russia has engaged in widespread and pervasive interference in democratic elections across the Council of Europe and beyond. Its aggressive tactics include weaponising disinformation to undermine democratic institutions, deliberate cyber-attacks against key State entities, including election infrastructure, "hack and leak" operations, and the use of "cyber troops" and "troll farms" to manipulate public discourse and to sow discord between social groups. The applicants contend that despite the existence of credible allegations that Russia sought to interfere in the United Kingdom's democratic processes, the respondent State neither investigated those allegations nor put in place an effective legal and institutional framework to protect against the risk of such interference.

THE FACTS

2. The applicants, who were born in 1960, 1960 and 1973, respectively, live in London. They were represented by Mr T.W. Short of Leigh Day, a firm of solicitors based in London.

3. The Government were represented by their Agent, Mr T. Geron of the Foreign, Commonwealth and Development Office.

4. The facts of the case may be summarised as follows.

I. BACKGROUND TO THE CASE

5. In February 2019 the House of Commons Digital, Culture, Media and Sport Committee ("DCMS") published a report entitled "Disinformation and 'fake news'" (see paragraphs 37-40 below). A further report by the Intelligence and Security Committee of Parliament ("ISC"), entitled "Russia" (see paragraphs 41-51 below), was sent to the Prime Minister in October 2019 and published in July 2020.

II. THE APPLICANTS' JUDICIAL REVIEW APPLICATION

6. The applicants were elected as Members of Parliament ("MPs") in the general election held on 12 December 2019. The first and second applicants did not stand in the next general election, held on 4 July 2024, and the third applicant lost his seat.

7. The applicants believed that the DCMS and ISC reports, together with the public response by the Government to the ISC report (see paragraphs 52-54 below), provided credible evidence of interference by Russia in the 2014 referendum on Scottish Independence ("the Scottish independence referendum"), the 2016 European Union membership referendum ("the EU referendum"), and the 2019 general election.

8. The applicants, together with two life peers and a non-profit organisation, sought permission to challenge, by way of judicial review, the Prime Minister's decision not to, and/or his ongoing failure to, direct an independent investigation into Russian interference with the country's democratic processes. They argued that in light of the ISC report this failure was in breach of the investigative obligation inherent in Article 3 of Protocol No. 1 to the Convention. They further challenged what they described as "the absence of an effective legal framework to ensure 'conditions which will ensure the free expression of the opinion of the people' as required by Article 3 of Protocol No. 1". Finally, they argued that the Prime Minister had failed to act compatibly with his public law duties in failing to establish a public inquiry.

A. Refusal of permission on the papers

9. On 12 April 2021 the applicants' application for permission to apply for judicial review was refused on the papers. The High Court judge noted at the outset that the grounds of challenge touched on core State functions and/or the exercise of State sovereignty. Under conventional principles of judicial review the courts should stand back from interference in such cases save where particular legal rights were engaged. That was not the case here, since none of the applicants' rights had been breached in any election or referendum.

10. In respect of the applicants' first ground, the High Court judge did not consider it arguable that Article 3 of Protocol No. 1 required the Prime Minister to undertake an independent investigation. With regard to past events, the imposition of such a duty would engage the courts in a highly politicised and contested exercise. With regard to future events, it was for the Prime Minister and not the courts to decide whether or not an independent investigation was required to ensure the free expression of the opinion of the people in forthcoming elections.

11. For the High Court judge the challenge to the legal framework was a matter of policy on which the court would not adjudicate.

12. Finally, the judge did not consider the decision not to establish a public inquiry to be irrational. She based her reasoning on the Prime Minister's summary grounds of resistance, which

indicated, *inter alia*, that Russia's actions had been the subject of a detailed report by the ISC (see paragraphs 41-51 below), and that wider public policy issues – such as the approach to disinformation and the use of social media – were the subject of ongoing policy development and public consultation. There was no evidence that any Russian activity had had any impact on the effectiveness of the right to vote, or on the outcome of any election. Moreover, a public inquiry did not have investigatory powers of the type that the police and Intelligence Agencies had. Given that the complaint was that there existed little evidence of successful Russian interference because insufficient investigative efforts had been made to collect that evidence, a public inquiry would not be able to fill that gap, if it existed.

13. The judge reached no conclusive view on the issue of standing, as the matter was "complex".

B. Renewed application for permission to apply for judicial review

14. The application for permission was renewed on the Convention rights' grounds only. It was refused by the High Court on 22 June 2021.

15. The High Court judge agreed that there was "no basis for the contention that the interference relied on affected the existence or exercise of any person's right to vote or right to stand as a candidate in an election" and did not consider it arguable that any legal obligation existed under Article 3 of Protocol No. 1. He gave detailed reasons, by reference to the Court's case-law, for reaching this conclusion.

16. Under the second ground, the applicants had argued that the domestic legal framework was in breach of Article 3 of Protocol No. 1 because:

1. There was no legal entity with the legal responsibility to prevent and combat foreign interference in elections;
2. There was no legal obligation for online political advertisements to indicate their source, who had paid for them, and their country of origin;
3. There was no legal requirement for social media companies to cooperate with the Security and Intelligence Agencies where it was suspected that a hostile foreign State may be covertly running a campaign;
4. There was no ban on foreign donations to political parties or election campaigns;
5. There was no obligation on foreign State agents, or others who represented the interests of foreign powers, to register as such in the United Kingdom.

17. The judge considered these complaints to be an assertion that there had been a failure to legislate, which fell outside the scope of section 6 of the Human Rights Act 1998 (see paragraph 19 below). In any event, the judge stated that the complaints were unarguable as Article 3 of Protocol No. 1 did not give rise to such specific obligations. It did not seek to prescribe the detailed structure or shape of electoral laws, and the Court had gone to significant lengths to emphasise the extent of the States' margin of appreciation when establishing such laws.

C. Application to Court of Appeal for permission to appeal

18. On 27 September 2021 the Court of Appeal refused the applicants' application for permission to appeal on the basis that their claim had no real prospect of success, and there was no other compelling reason to hear the appeal.

RELEVANT LEGAL FRAMEWORK AND PRACTICE

I. RELEVANT DOMESTIC LAW

A. Legislation

1. *The Human Rights Act 1998 ("HRA")*

19. Pursuant to section 6(1) of the HRA, it was unlawful for a public authority to act in a way which was incompatible with a Convention right. However, according to section 6(6) an "act" did not include a failure to introduce in, or lay before, Parliament a proposal for legislation, or a failure to make any primary legislation or remedial order.

2. *The Inquiries Act 2005*

20. The Inquiries Act 2005 provided a statutory framework for Government Ministers to order inquiries to be held where events had occurred which caused, or which were capable of causing, public concern. Inquiries were not adversarial in nature; rather, they were an inquisitorial process aimed at establishing the truth. They were usually conducted in public, and the chairman's report was usually published, although in certain circumstances – for example, where there was a risk to national security – public access and the disclosure of evidence could be restricted and certain material in the report could be withheld from publication.

3. *The Elections Act 2022*

21. Electoral law in the United Kingdom is comprised of primary and secondary legislative material governing elections and referendums.

22. Until recently, the Representation of the People Acts 1983 and 2000 ("RPA 1983" and "RPA 2000") and the Political Parties, Elections and Referendums Act 2000 ("PPERA") were the key pieces of primary legislation. Among other things, they provided that any donations made to political parties, recognised third-parties, regulated donees (being members of registered political parties, holders of relevant elective office and members associations subject to controls on the donations and loans that they can accept) and candidates could only be made by United Kingdom-based or otherwise eligible sources. Donations from impermissible sources, including ineligible foreign donations, were prohibited.

23. The Elections Act 2022 ("the 2022 Act") received Royal Assent on 28 April 2022. It amended the law about political finance. In particular, it clarified the rules on notional spending and restricted third-party spending to United Kingdom-based entities and eligible overseas electors only. It also increased transparency around third-party campaigning, and introduced a statutory duty for the Electoral Commission to produce guidance on the operation of Part 6 of PPERA, which concerned controls relating to third-party national election campaigns.

24. By virtue of section 110 of the RPA 1983 and section 143 of PPERA, printed material produced during an election campaign had to include an imprint providing information about who had produced the material and on behalf of whom they promoted it. Part 6 of the 2022 Act introduced a new requirement for digital campaigning material to display a digital imprint, with the name and address of the promoter of the material or any person on behalf of whom the material was being published (and who was not the promoter).

4. *The National Security Act 2023*

25. The National Security Act 2023 ("the NSA 2023"), which received Royal Assent on 11 July 2023, brought together a suite of new measures to protect the United Kingdom's national security, the safety of the British public and the United Kingdom's vital interests from the hostile activities of foreign States.

26. More particularly, the NSA 2023 created new offences and accompanying police powers to capture harmful activity around sites that were critical to the safety or interests of the United Kingdom; explicitly criminalised assisting a foreign intelligence service in carrying out activities in the United Kingdom or overseas where such conduct was prejudicial to the United Kingdom's safety and interests; established a new offence of sabotage designed to capture State-linked saboteurs who acted in a way that was prejudicial to the United Kingdom's safety or interests by causing damage, including through cyber-attacks, to assets (including critical infrastructure, electronic systems and information); established a new offence of foreign interference where conduct was intended to have a specified negative effect and certain conditions were satisfied; increased the maximum custodial penalties for certain election-related offences that were carried out for or on behalf of, or with the intention to benefit, a foreign power; and replaced the existing acts preparatory offence under the Official Secrets Act 1920 with a new offence to ensure that it could effectively target harmful preparatory State threats activity.

27. Part 4 of the NSA 2023 introduced a Foreign Influence Registration Scheme to strengthen the resilience of the United Kingdom political system against covert foreign influence and to provide greater assurance around the activities of specified foreign powers or entities.

5. The Online Safety Act 2023

28. The Online Safety Act 2023 ("the OSA 2023"), which received Royal Assent on 26 October 2023, established a new regulatory regime holding tech companies accountable to an independent regulator. It addressed misinformation and disinformation where it constituted illegal content or content harmful to children, and set out a list of priority offences reflecting the most serious and prevalent illegal content and activity, against which companies had to take proactive measures. The offence of foreign interference introduced by the NSA 2023 (see paragraph 26 above) was deemed to be a "priority offence".

B. Regulation and oversight

1. The Election Court

29. According to section 120 of the RPA 1983 (see paragraph 22 above), petitions against the outcome of elections, or the outcome of an election campaign, can be brought before the Election Court. Section 157 of the RPA 1983 allows decisions of the Election Court to be appealed to the Court of Appeal on a question of law.

2. The Electoral Commission

30. The Electoral Commission is an independent statutory body responsible for overseeing elections and regulating political finance in the United Kingdom. It seeks to promote public confidence in the democratic process and ensure its integrity. It has extensive powers and responsibilities to oversee compliance with electoral law, as well as to issue public reports on the conduct of elections. It was set up under PPERA (see paragraph 22 above) to be independent of Government. It is directly accountable to Parliament.

31. Under Parts V and VI of PPERA (see paragraph 22 above), the Electoral Commission publishes details of all payments made by political parties and registered third-party campaigners during the regulated period in the run-up to a parliamentary election. It also publishes online donations to political parties above 7,500 British Pounds (GBP).

3. The Counter Disinformation Unit

32. The Counter Disinformation Unit ("CDU"), now known as the National Security Online Information Team ("NSOIT") was set up in 2019 and currently sits within the Department for Science, Innovation and Technology. It leads the domestic operational and policy response for countering disinformation across Government. It brings together monitoring and analysis capabilities for major elections, key national events and acute information incidents, such as the Russian information operations during the war in Ukraine and Covid 19. It also proactively monitors for harmful narratives that threaten the United Kingdom, and co-ordinates with Government departments to deploy the appropriate response to mis/disinformation. This could involve a direct rebuttal on social media, awareness raising campaigns to promote the facts or, in cases where platforms' terms of service may have been violated, referring content to the relevant platform for consideration.

33. According to a factsheet published by the United Kingdom Government on the CDU, disinformation is defined as the deliberate creation and spreading of false and/or manipulated information that is intended to deceive and mislead people, either for the purposes of causing harm, or for political, personal or financial gain. Misinformation, on the other hand, is the inadvertent spread of false information.

4. The "Defending Democracy" Taskforce

34. In November 2022 the Government launched its Defending Democracy Taskforce. Its stated aim was to "protect the democratic integrity of the UK" as an "enduring government function with particular focus on foreign interference".

35. It works with local councils, police forces and global tech companies to:

1. ensure that electoral processes and infrastructure are secure and resilient;
2. ensure elected officials are protected "at all levels" from physical, cyber, and additional threats; and
3. counter disinformation efforts aimed at "disrupting our national conversation and skewing our democratic processes".

36. The Taskforce works across Government and with Parliament, the United Kingdom intelligence community, the devolved administrations, local authorities, the private sector and civil society with the aim of building resilience across all levels of the United Kingdom's democratic system. It reports to the National Security Council, which is a Cabinet Committee chaired by the Prime Minister.

C. Domestic reports on the impact of disinformation

1. The final report by the House of Commons Digital, Culture, Media and Sport Committee ("DCMS") entitled Disinformation and 'fake news'

37. The DCMS is a cross-party committee of MPs appointed by the House of Commons to examine the expenditure, administration and policy of the Department for Digital, Culture, Media and Sport and its associated public bodies.

38. Over the course of eighteen months it conducted an inquiry on disinformation, covering, *inter alia*, how individuals' political choices might be affected and influenced by online information and interference by malign forces in political elections in the United Kingdom. Its report was published in February 2019.

39. Under the heading, "Foreign influence in political campaigns", the report stated:

"There has been clear and proven Russian influence in foreign elections, and we highlighted evidence in our Interim Report of such attempts in the EU Referendum."

40. Having specific regard to Russian interference in domestic elections, the report continued:

"As we said in our Interim Report, Prime Minister Theresa May accused Russia of meddling in elections, and planting disinformation, in an attempt to 'weaponise information' and sow discord in the West. In its response to the Report, the Government stated that, following the nerve agent attack in Salisbury in March 2018, the Government had 'judged the Russian state promulgated at least 38 false disinformation narratives around this criminal act'. However, the Government made it clear that 'it has not seen evidence of successful use of disinformation by foreign actors, including Russia, to influence UK democratic processes'.

When the Secretary of State was questioned in oral evidence over what constitutes 'successful', Rt Hon Jeremy Wright MP, responded: 'We have seen nothing that persuades us that Russian interference has had a material impact on the way in which people choose to vote in elections. It is not that they have not tried, but we have not seen evidence of that material impact'. It is surely a sufficient matter of concern that the Government has acknowledged that interference has occurred, irrespective of the lack of evidence of impact. The Government should be conducting analysis to understand the extent of Russian targeting of voters during elections.

The Government also cannot state definitively that there was 'no evidence of successful interference' in our democratic processes, as the term 'successful' is impossible to define in retrospect. There is, however, strong evidence that points to hostile state actors influencing democratic processes. Cardiff University and the Digital Forensics Lab of the Atlantic Council have both detailed ways in which the Kremlin attempted to influence attitudes in UK politics.

Kremlin-aligned media published significant numbers of unique articles about the EU referendum. 89 Up researchers analysed the most shared of the articles, and identified 261 with a clear anti-EU bias to the reporting. The two main outlets were RT and Sputnik, with video produced by Ruptly. The articles that went most viral had the heaviest anti-EU bias. The social reach of these anti-EU articles published by the Kremlin-owned channels was 134 million potential impressions, in comparison with a total reach of just 33 million and 11 million potential impressions for all content shared from the Vote Leave website and Leave.EU website respectively. The value for a comparable paid social media campaign would be between £1.4 and 4.14 million.

...

Ben Nimmo, from the Digital Forensics Lab of the Atlantic Council, has detailed attempts to influence attitudes to the Scottish Referendum, for instance, which included a Russian election observer calling the referendum not in line with international standards, and Twitter accounts calling into question its legitimacy. The behaviour of these accounts, Mr Nimmo argues, is pro-Kremlin, and consistent with the behaviour of accounts known to be run by the so-called 'troll factory' in St. Petersburg, Russia, during the United States 2016 presidential election and beyond. However, it is not possible to determine from open sources whether some or all of the accounts are independent actors, or linked to Russian information operations.

...

The Government has been very ready to accept the evidence of Russian activity in the Skripal case, an acceptance justified by the evidence. However, it is reluctant to accept evidence of interference in

the 2016 Referendum in the UK. If the Government wishes the public to treat its statements on these important matters of national security and democracy seriously, it must report the position impartially, uninfluenced by the political implications of any such report.

In common with other countries, the UK is clearly vulnerable to covert digital influence campaigns and the Government should be conducting analysis to understand the extent of the targeting of voters, by foreign players, during past elections. We ask the Government whether current legislation to protect the electoral process from malign influence is sufficient. Legislation should be in line with the latest technological developments, and should be explicit on the illegal influencing of the democratic process by foreign players. We urge the Government to look into this issue and to respond in its White Paper."

2. The report by the Intelligence and Security Committee of Parliament ("ISC") entitled "Russia"

41. The ISC is a statutory committee that has responsibility for oversight of the United Kingdom Intelligence Community. Its nine Members, who are drawn from both Houses of Parliament, are appointed by the Houses of Parliament, having been nominated by the Prime Minister in consultation with the Leader of the Opposition.

42. Throughout 2018 the ISC conducted a major Inquiry which covered various aspects of the Russian threat to the United Kingdom, together with an examination of how the United Kingdom Government had responded. A report was completed on 17 October 2019 and, having already been cleared by the Security and Intelligence Agencies, was sent to the Prime Minister. On 5 November 2019 – the day before Parliament was dissolved ahead of the 2019 election – the Chair of the ISC asked the Prime Minister, in Parliament, if he would make a statement on his refusal to give clearance to the report. In doing so, he referred to a long-standing agreement that the Prime Minister would endeavour to respond to such reports within ten days. In response, he was informed by the Minister for Europe and the Americas that scrutiny of such a sensitive report took time. The report was eventually presented to Parliament and published with redactions (represented by "***") on 21 July 2020. Although the report was supplemented by an annex, that annex has not yet been published, "in view of the current Russian threat".

43. The report found that:

"It is clear that Russia currently poses a significant threat to the UK on a number of fronts – from espionage to interference in democratic processes, and to serious crime. The question is how that has happened – and what the Intelligence Community is now doing to tackle it."

44. In the specific context of interference in democratic processes, the report noted:

"The spreading of disinformation (by which we mean the promotion of intentionally false, distorting or distracting narratives) and the running of 'influence campaigns' are separate but interlinked subjects. An influence campaign in relation to an election, for example, may use the spreading of disinformation, but may also encompass other tactics such as illicit funding, disruption of electoral mechanics or direct attacks on one of the campaigns (such as 'hack and leak').

...

In terms of the direct threat to elections, we have been informed that the mechanics of the UK's voting system are deemed largely sound: the use of a highly dispersed paper-based voting and counting system makes any significant interference difficult, and we understand that GCHQ [Government Communication Headquarters, the United Kingdom's intelligence, security and cyber

Agency] has undertaken a great deal of work to help ensure that the online voter registration system is safe."

45. Nonetheless, the report continued:

"The UK is clearly a target for Russia's disinformation campaigns and political influence operations and must therefore equip itself to counter such efforts.

...

... [W]e note that – as with so many other issues currently – it is the social media companies which hold the key and yet are failing to play their part; DCMS informed us that ***. The Government must now seek to establish a protocol with the social media companies to ensure that they take covert hostile state use of their platforms seriously, and have clear timescales within which they commit to removing such material. Government should 'name and shame' those which fail to act. Such a protocol could, usefully, be expanded to encompass the other areas in which action is required from the social media companies, since this issue is not unique to Hostile State Activity. This matter is, in our view, urgent and we expect the Government to report on progress in this area as soon as possible."

46. By way of a case study, the report considered the EU referendum, since there had been widespread public allegations that Russia had sought to influence it. According to the report:

"The impact of any such attempts would be difficult – if not impossible – to assess, and we have not sought to do so. However, it is important to establish whether a hostile state took deliberate action with the aim of influencing a UK democratic process, irrespective of whether it was successful or not.

Open source studies have pointed to the preponderance of pro-Brexit or anti-EU stories on RT and Sputnik, and the use of 'bots' and 'trolls', as evidence of Russian attempts to influence the process."

47. The report also noted the existence of "credible open source commentary" suggesting that Russia undertook influence campaigns in relation to the Scottish independence referendum.

48. Concerning the Government's response to allegations of Russian interference in its democratic processes, the report indicated:

"The written evidence provided to us appeared to suggest that [the Government] had not seen or sought evidence of successful interference in UK democratic processes or any activity that has had a material impact on an election, for example influencing results. ***. ***. This focus on *** indicates that open source material (for example, the studies of attempts to influence the referendum using RT and Sputnik, or social media campaigns referred to earlier) was not fully taken into account. Given that the Committee has previously been informed that open source material is now fully represented in the Government's understanding of the threat picture, it was surprising to us that in this instance it was not.

Whilst it may be true that some issues highlighted in open source did not require the secret investigative capabilities of the intelligence and security Agencies or were at the periphery of their remits, the Agencies nonetheless have capabilities which allow them to 'stand on the shoulders' of open source coverage: for example, GCHQ might attempt to look behind the suspicious social media accounts which open source analysis has identified to uncover their true operators (and even disrupt their use), or SIS [Secret Intelligence Service, otherwise known as MI6] might specifically task an

agent to provide information on the extent and nature of any Russian influence campaigns. However, we have found *** which suggests that ***. ***.

(iii) Lack of retrospective assessment

We have not been provided with any post-referendum assessment of Russian attempts at interference, ***. This situation is in stark contrast to the US handling of allegations of Russian interference in the 2016 presidential election, where an intelligence community assessment was produced within two months of the vote, with an unclassified summary being made public. Whilst the issues at stake in the EU referendum campaign are less clear-cut, it is nonetheless the Committee's view that the UK Intelligence Community should produce an analogous assessment of potential Russian interference in the EU referendum and that an unclassified summary of it be published.

***. Even if the conclusion of any such assessment were that there was minimal interference, this would nonetheless represent a helpful reassurance to the public that the UK's democratic processes had remained relatively safe."

49. The report noted that following the end of the Cold War, the operational effort allocated to countering Russian Hostile State Activity decreased. The report continued:

"We fully recognise the very considerable pressures on the Agencies since 9/11, and that they have a finite amount of resource, which they must focus on operational priorities. Nevertheless, reacting to the here and now is inherently inefficient and – in our opinion – until recently, the Government had badly underestimated the Russian threat and the response it required."

50. The Intelligence Agencies had informed the ISC that the DCMS had primary responsibility for disinformation campaigns, and that the Electoral Commission (see paragraphs 30-31 above) had responsibility for the overall security of democratic processes. However, the DCMS told the ISC that its function was largely confined to the broad Government policy regarding the use of disinformation rather than an assessment of, or operations against, hostile State campaigns. According to the ISC:

"DCMS is a small Whitehall policy department and the Electoral Commission is an arm's length body; neither is in the central position required to tackle a major hostile state threat to our democracy. Protecting our democratic discourse and processes from hostile foreign interference is a central responsibility of Government, and should be a ministerial priority."

51. The report also considered whether the Intelligence Community had all the powers and tools it needed to counter Russian Hostile State Activity. Under the heading "Protecting democracy" it stated:

"The [DCMS] Select Committee has already asked the Government 'whether current legislation to protect the electoral process from malign interference is sufficient. Legislation should be in line with the latest technological developments'. We note that physical interference in the UK's democratic processes is less likely given the use of a paper-based system – however, we support the DCMS Select Committee's calls for the Electoral Commission to be given power to 'stop someone acting illegally in a campaign if they live outside the UK'.

Separately, there is the question of influence over our democratic processes. Questions have been raised over whether electoral law is sufficiently up to date, given 'the move from physical billboards to online, micro-targeted political campaigning'. We note – and, again, agree with the DCMS Select

Committee – that 'the UK is clearly vulnerable to covert digital influence campaigns'. In this respect, we have already questioned whether the Electoral Commission has sufficient powers to ensure the security of democratic processes where hostile state threats are involved; if it is to tackle foreign interference, then it must be given the necessary legislative powers."

3. The Government's public response to the ISC "Russia" report

52. In July 2020 the Government published a public response to the ISC report. It stated that:

"The UK's free and open democracy is one of our nation's greatest strengths. However, we know that certain states seek to exploit our open system to sow division and undermine trust in our democracy, and those of our allies, through disinformation, cyber-attacks and other methods. We have made clear that any foreign interference in the UK's Democratic processes is completely unacceptable. It is, and always will be, an absolute priority to protect the UK against foreign interference, whether from Russia or any other state.

We have worked with industry, civil society and international partners to implement robust systems to secure our Democratic processes and deter attempts to interfere in it. This work is undertaken with the utmost regard for the freedom of the press, political and parliamentary discourse and freedom of speech. We will always balance the need to secure our Democracy with our duty to uphold our values."

53. The Government acknowledged that it was "almost certain that Russian actors sought to interfere in the 2019 General Election through the online amplification of illicitly acquired and leaked Government documents." The response also referred to "several incidents during the 2019 General Election including distributed denial of service attacks against political parties, and suspicious emails received by candidates." However, the Government had seen "no evidence of successful interference in the EU Referendum".

54. The response continued:

"Whilst there is no evidence of a broad spectrum Russian campaign against the election, any attempt to interfere in our democratic processes is completely unacceptable. There is an ongoing criminal investigation and it would be inappropriate for us to say anything further at this point.

...

The Intelligence and Security Agencies produce and contribute to regular assessments of the threat posed by Hostile State Activity, including around potential interference in UK democratic processes. We keep such assessments under review and, where necessary, update them in response to new intelligence, including during democratic events such as elections and referendums. Where new information emerges, the Government will always consider the most appropriate use of any intelligence it develops or receives, including whether it is appropriate to make this public. Given this long standing approach, a retrospective assessment of the EU Referendum is not necessary."

4. National Cyber Security Centre ("NCSC") Annual Review 2023

55. The NCSC, which is part of Government Communication Headquarters ("GCHQ", the United Kingdom's intelligence, security and cyber Agency), was launched in October 2016 to act as a bridge between industry and government, and provide a unified source of advice, guidance and support on cyber security, including the management of cyber security incidents. It works collaboratively with other law enforcement agencies, defence agencies, the United Kingdom's Intelligence and Security Agencies, and international partners.

56. On the issue of election interference, the NCSC said the following in its 2023 annual review:

"Russian attempts to manipulate democratic institutions

It is no secret that Russia seeks to weaken and divide their adversaries by interfering in elections using mis and dis-information, cyber attacks, and other methods.

The UK government assesses that it is almost certain that Russian actors sought to interfere in the 2019 general election. In the coming months, with UK and US elections on the horizon we can expect to see the integrity of our systems tested again.

Protecting our democratic and electoral processes against foreign interference, whether from Russia or any other state, is and always will be an absolute priority for the NCSC and we will continue to support the government's critical work in this area.

...

Case study: Defending our democracy in a new digital age –
at the ballot box and beyond

...

With elections on the horizon, including a general election, and with people around the world set to go to the polls from Belgium to the US in the next year, the UK and its allies cannot be complacent to the threat of foreign cyber interference and attempts at influencing our democratic processes. The NCSC is working with our allies around the world to share insights and approaches to help improve collective cyber resilience of global democracy.

Defending democracy is a critical part of the NCSC's mission as it gets to the heart of what it means to keep the UK safe, and to act responsibly, in cyberspace.

As part of a cross-government effort, alongside partners in industry, civil society and others, we are working to protect the values at the foundation of our society.

Responding to threats

Protecting our democracy in cyberspace requires a continuous effort as the cyber threat to the UK's democratic institutions and processes is significant and comes from many malicious actors.

Over the past year, the NCSC has surged its efforts to advise on the smooth running of local elections, political party leadership contests and once-in-a-generation constitutional events such as the Coronation of His Majesty the King.

We have supported a range of entities involved in the democratic process with their responses to cyber incidents, ranging from phishing attacks to more sophisticated compromises.

And we have provided longer-term guidance for improving resilience, both across supply chains that underpin the functioning of key services and to individuals active in our democracy, such as politicians, where we have seen them being targeted.

Looking ahead

The next general election is set to take place before the end of January 2025, with local and mayoral elections scheduled next May. The NCSC is already working with key stakeholders across government, UK parliament, the devolved administrations and legislatures, and industry to prepare for it.

When the UK goes to the polls, the act of casting your vote is completed using pencil and paper, significantly reducing the chances of a cyber actor affecting the integrity of the results.

However, the act of voting marks the end of the sprint, as a significant amount of cyber-resilience building needs to take place before this to secure the services which support our elections and the integrity of an open public discourse.

The government's Defending Democracy Taskforce has established the Joint Election Security Preparedness unit (JESP), which takes overall responsibility for coordinating electoral security and drives the government's election preparedness.

It plays a central role in convening government departments, the devolved administrations and legislatures, and security resources to ensure our systems and processes are resilient.

And for those who have a direct role to play, the NCSC has existing defending democracy guidance, which is currently being refreshed. We strongly encourage following the recommended steps to ensure online protections are in place.

...

Collective action

Defending the UK's democratic institutions and processes is a priority for the NCSC. However, it is not something we can achieve alone.

It requires a collective effort across the whole of society, including industry and in partnership with allies, to defend our values and make the UK an unattractive environment for hostile actors.

Our democracy is founded on the principle of participation; every member of the public across the four nations of the UK has a stake, and everyone has a role to play in defending it.

By acting now to strengthen systems and accounts – rather than waiting until an incident occurs or an election is called – we can help make our society safer online."

57. In its 2024 annual review, the NCSC noted:

"The 2024 general election took place in a complex information environment. The NCSC partnered with colleagues across government to offer expert technical advice on how to protect against and respond to information-based incidents. This included using our expertise in exercising to test a number of scenarios and our collective readiness to respond to any incidents, as well as participating in JESP's Election Security Exercise Programme."

5. Independent Reviewer of Terrorism and State Threat Legislation; report of 19 May 2025

58. The Independent Reviewer of Terrorism Legislation is a person wholly independent of Government, appointed by the Home Secretary and by the Treasury for a renewable three-year term. He is tasked with reporting to the Home Secretary and to Parliament on the operation of counter-terrorism law in the United Kingdom. These reports are laid before Parliament to inform the public and political debate.

59. The purpose of this independent review was to examine whether there were tools available in terrorism legislation which should be emulated or adapted to address State-based security threats to the United Kingdom. It was separate from the Independent Reviewer's much longer annual review of State Threat legislation which has now been submitted to the Home Office, and which considers in detail its effectiveness, fairness, and any potential pitfalls.

60. The Independent Reviewer noted that the Terrorism Act 2000 did not cover the actions of State entities, and that there were terrorism powers that were not currently replicated in existing State Threat legislation. He made the following recommendations:

- Ability to issue Statutory Alert and Liability Threat Notices against Foreign Intelligence Services, an equivalent to proscription under the Terrorism Act 2000. This power, available against State entities, and private entities acting as Foreign Intelligence Services, would be added to the NSA.
- Creation of additional criminal offences for individuals who invite support for or display the insignia of the Foreign Intelligence Service in question.
- Application of the acts preparatory offence to certain State Threat activity done in the UK where the intended target is overseas.
- Police to be given power to erect cordons in State Threat investigations.
- Consideration be given to a power to stop and search individuals without suspicion in high threat situations, or locations such as the premises of a known State Threat target.
- Power in limited circumstances to carry out post-charge interviews in State Threat criminal investigations.
- Police to be given the power to seize passports on the basis of suspected foreign power threat activity, as currently exists in terrorism cases.
- The relocation power should be available in a wider range of State Threat Prevention and Investigation Measures under Part 2 of the National Security Act 2023.
- Amendment to the Serious Crime Act 2007 to allow police to apply directly to the High Court for Serious Crime Prevention Orders in State Threat cases.

61. The Independent Reviewer considered that the Government needed to do even more to warn the public about the risk posed by the most dangerous Foreign Intelligence Services. Whilst few Foreign Intelligence Services would ever act openly, the fact that such organisations actively aspired to damage national security should be prominently exposed for public consumption.

II. INTERNATIONAL LAW AND PRACTICE

A. United Nations

1. *The League of Nations: International Convention Concerning the Use of Broadcasting in the Cause of Peace*

62. The League of Nations recognised the risks posed by disinformation. By virtue of the International Convention Concerning the Use of Broadcasting in the Cause of Peace, which was signed in Geneva on 23 September 1936 (LNTS No 4319), the High Contracting Parties undertook to prohibit and stop the broadcasting within their respective territories of any transmission which would be to the detriment of good international understanding (by, *inter alia*, statements the incorrectness of which were or ought to have been known to the persons responsible for the broadcast) or which would incite the population to acts incompatible with the internal order or the security of a territory of a High Contracting Party and to rectify them at the earliest possible moment by the most effective means.

2. *Joint declaration on freedom of expression and "fake news", disinformation and propaganda (March 2017)*

63. This joint declaration was issued by the United Nations ("UN") Special Rapporteur on Freedom of Opinion and Expression, the Organization for Security and Co-operation in Europe (""OSCE") Representative on Freedom of the Media, the Organization of American States ("OAS") Special Rapporteur on Freedom of Expression and the African Commission on Human and Peoples' Rights

("ACHPR") Special Rapporteur on Freedom of Expression and Access to Information. Together, they noted the growing prevalence of disinformation and propaganda in legacy and social media, fuelled by both States and non-State actors, and expressed concern that disinformation and propaganda were often designed and implemented so as to mislead a population, as well as to interfere with the public's right to know and the right of individuals to seek, receive and impart information and ideas of all kinds.

3. *Office of the High Commissioner for Human Rights: 2021 Handbook on International Human Rights Standards on Elections*

64. This 2021 handbook made the following remarks about the impact of disinformation on elections:

"Impact of big data manipulation and social media on elections

New challenges to elections have arisen in the digital age, notably information disorder and big data manipulation. While the human right to impart information and ideas is not limited to 'correct' statements, and protects information and ideas that may shock, offend and disturb, widespread disinformation may pose significant threats to the right to political participation, both in relation to the right to participate in public affairs and to stand for elections and vote. Social media platforms have become key for political actors to disseminate disinformation, often helped by the preference of content curation algorithms for sensationalist content and the possibility to micro-target political advertising. In the context of electoral processes, social media may be instrumentalized to influence the outcomes of elections by discrediting candidates and political parties, providing incorrect information about the voting process (vote suppression) and seeking to influence the voting choices of particular segments of society that may be targeted based on patterns suggested by the processing of personal data and social media activity.

Disinformation may result in prerequisite rights to free and genuine elections being violated. For example, hate speech and discrimination can be amplified by online disinformation campaigns and may in turn lead to risks to the security of person and hate crimes. Freedom of expression and access to information may also be affected if a voter only has access to news through one social media platform that predominantly or only contains disinformation. Disseminating disinformation may lead to reducing understanding among people with different opinions or backgrounds and exacerbating polarization, playing on and distorting people's negative views of others. It can be used to splinter and manipulate public discourse, depriving voters of critical information for their decision-making.

While disinformation constitutes a real challenge in the electoral context, States should refrain from general and ambiguous prohibition of the dissemination of information, such as 'falsehoods' or 'non-objective information'. Such terms do not adequately describe the content that is prohibited. As a result, they provide the authorities with a broad remit to censor the expression of unpopular, controversial or minority opinions, as well as criticism of the Government and politicians in the media and during electoral campaigns. Human rights experts have recommended that approaches to combat disinformation should avoid criminalization and be instead evidence-based and tailored to the proven or documented impacts of disinformation and propaganda. These measures could include the promotion of independent fact-checking mechanisms, the provision of support for

independent and diverse public service media outlets, public education and digital literacy campaigns."

4. *Human Rights Council Resolution 49/21 of 1 April 2021 on the role of States in countering the negative impact of disinformation on the enjoyment and realization of human rights*

65. In this Resolution the Human Rights Council said the following:

"...*Emphasizing* further that disinformation is a threat to democracy that can suppress political engagement, engender or deepen distrust towards democratic institutions and processes, and hinder the realization of informed participation in political and public affairs,

...

Expressing concern about the dissemination of disinformation by both traditional and digital means, and that digital technology can be used to create, disseminate and amplify disinformation by State and non-State actors for political, ideological or commercial motives at an alarming scale, speed and reach,

...

Stressing that condemning and countering disinformation should not be used as a pretext to restrict the enjoyment and realization of human rights or to justify censorship, including through vague and overly broad laws criminalizing disinformation, and that all policies or legislation undertaken to counter disinformation must be in compliance with States' obligations under international human rights law, including the requirement that any restrictions on freedom of expression comply with the principles of legality and necessity,

1. *Affirms* that disinformation can negatively affect the enjoyment and realization of all human rights, and that States play a central role in countering disinformation;

2. *Calls* upon States to ensure that their responses to the spread of disinformation comply with international human rights law and that their efforts to counter disinformation promote, protect and respect individuals' freedom of expression and freedom to seek, receive and impart information, as well as other human rights;

3. *Urges* States to facilitate an environment supportive of countering disinformation through multidimensional and multi-stakeholder responses that are in compliance with international human rights law, including through enhanced cooperation with international organizations, civil society, the media, the private sector and other stakeholders;

4. *Invites* States to encourage business enterprises, including social media companies, to address disinformation while respecting human rights, including through the review of business models, in particular the role of algorithms and ranking systems in amplifying disinformation, enhancing transparency, enforcing all applicable legal protections for users and encouraging due diligence in line with the Guiding Principles on Business and Human Rights;

5. *Calls* upon all States to refrain from conducting or sponsoring disinformation campaigns domestically or transnationally for political or other purposes, and encourages them to condemn such acts;

6. *Commits* to the promotion of international cooperation to counter the negative impact of disinformation on the enjoyment and realization of human rights; ..."

5. *Disinformation and freedom of opinion and expression – Report of the UN Special Rapporteur on Freedom of Opinion and Expression on the promotion and protection of the right to freedom of opinion and expression (13 April 2021)*

66. The Special Rapporteur acknowledged that disinformation was a complex, multifaceted phenomenon with serious consequences, including destroying people's trust in democratic institutions. However, while disinformation was problematic, so too were the responses of States. Laws and policies were often being made with sub-optimal knowledge of online harm, and without adequate data, research or public consultations. States had resorted to disproportionate measures such as Internet shutdowns and vague and overly broad laws to criminalize, block, censor and chill online speech and shrink civic space. These measures were not only incompatible with international human rights law but also contributed to amplifying misperceptions, fostering fear and entrenching public mistrust of institutions.

B. Council of Europe

1. *Resolution 2254 (2019) of the Parliamentary Assembly of the Council of Europe ("PACE"): Media freedom as a condition for democratic elections*

67. In this Resolution PACE recalled that free elections were a pillar of every democratic society, and that the electorate could not be said to have genuine freedom of choice if that choice was not a well-informed one. Consequently, the right to freedom of information and media freedom were essential preconditions of the right to free elections, in accordance with Article 3 of Protocol No. 1 to the Convention. It continued:

"3. Alongside the professional media, new media players have arrived on the scene: social media. They are having an increasing impact on the public, including during election campaigns: they enable political parties and candidates to pass on their messages 'directly' to the electorate, and are a means for their supporters to disseminate those messages.

4. In many countries, social media are not subject to the general regulations governing the media or to the specific rules that apply at election times. Moreover, the particular nature of online communication makes it difficult to apply to social media the principles which the professional media must respect. Most attempts at regulation have failed to yield convincing results of compliance; other attempts have been heavy-handed and have amounted to censorship. Furthermore, sites which have been closed down can respond by creating 'mirror sites' beyond national borders, which makes the sanctions adopted by domestic authorities less effective. There is also a lack of self-regulation by social media, which often disregard the conventions that have been widely accepted by the professional media.

5. Given the existing legal gaps, the various forms of malevolent online communication endanger the smooth and fair conduct of the electoral process and, ultimately, of democracy itself. Today, there is sufficient proof that autocratic regimes and anonymous stakeholders or interest groups use social media to manipulate public opinion with false news, co-ordinated disinformation campaigns, and trolls or bots to attack not only candidates in the opposing camp, but also human rights defenders, activists, civil society groups and journalists. Furthermore, even though recent research seems to show that social media users are exposed to more diverse information sources than those not using online sources, 'filter bubbles' and 'echo chambers' may hamper the potential benefits of

such positive exposure, compartmentalise information flows and undermine internet users' ability to think critically, thus reinforcing prejudices.

6. In order to respond effectively to these problems, member States should guarantee the right to information through independent media; in addition, they should implement effective strategies to protect the electoral process and democracy from the threat of information manipulation and undue propaganda through social media.

...

8. Accordingly, the Assembly calls on member States to review, where necessary, their regulatory frameworks governing media coverage of election campaigns, in order to bring them into line with Council of Europe standards, ...

9. Concerning more specifically the risks posed by disinformation and undue propaganda on the internet and social media for the smooth conduct of the electoral process, the Assembly calls on member States to:

9.1 refrain from disseminating or encouraging the dissemination on the internet of statements, communications or news which they know or can reasonably be expected to know to be disinformation or undue propaganda;

9.2 develop specific regulatory frameworks for internet content at election times and include in these frameworks provisions on transparency in relation to sponsored content published on social media, so that the public can be aware of the source that funds electoral advertising or any other information or opinion;

9.3 establish clear legal liability for social media companies which publish illegal content harmful to candidates or violate essential rules of media communication during election times;

9.4 ensure that sanctions provided for in relation to unlawful content are not diverted to force self-censorship of opponents' opinions and critical views, and limit the application of extreme measures such as the blocking of entire websites, IP addresses, ports or network protocols to the most serious cases, in full compliance with the strict conditions set out in Article 10 of the European Convention on Human Rights;

9.5 provide specific training for electoral management bodies and media regulators, so that their members can gain a better understanding of the new media environment, with a view to enhancing implementation of regulations on political communication via social media;

9.6 encourage all stakeholders – including internet intermediaries, media outlets, civil society and academia – to develop participatory initiatives to enable the general public to have a better understanding of the danger of disinformation and undue propaganda on the internet, and to seek together appropriate responses to these phenomena."

2. *PACE Resolution 2326 (2020): Democracy hacked? How to respond?*

68. In this Resolution PACE expressed concern about, *inter alia*, the spread of disinformation campaigns aimed at shaping public opinion and trends of foreign electoral interference and manipulation. In PACE's view, these represented a challenge for democracy, and in particular for the electoral processes throughout Council of Europe member States, affecting the right to freedom of expression, including the right to receive information, and the right to free elections.

69. According to PACE, in order to address disinformation challenges in the context of democratic elections, Governments of Council of Europe member States needed to:

1. recognise the transnational nature of the problem and enhance co-operation with internet intermediaries and social media operators;
2. enable voters to receive trustworthy information and become more informed and engaged;
3. break up the monopoly of technology companies controlling, to a great extent, citizen's access to information and data; and
4. consider updating national legislation in order to counter disinformation campaigns more effectively.

70. PACE therefore called on Council of Europe member States to implement a number of strategies from a European and global perspective which were targeted both at elections and candidates in elections as well as the political process more generally, and to create a model that includes co-responsibility and multiple regulatory and conflict-resolution approaches.

3. Other material from the Council of Europe on disinformation and electoral campaigns

(a) European Commission for Democracy Through Law (Venice Commission): The impact of the information disorder (disinformation) on elections (November 2018)

71. According to the author of this report,

"Today we are witnessing the parallel proliferation of information and its pollution at a global scale. The internet-based services have enriched and diversified news sources, facilitating individuals' access to information and their decisions on the most crucial matters in democracy, notably on the choice of their legislature. However, at the same time, a new era of information disorder (CoE Information Disorder Report, 2017) distorted the communication ecosystem to the point where voters may be seriously encumbered in their decisions by misleading, manipulative and false information designed to influence their votes. This environment potentially undermines the exercise of the right to free elections and creates considerable risks to the functioning of a democratic system."

72. As a consequence, the author believed that "[t]he guarantees of a level playing field aimed at ensuring fair, clean and clear campaigns are under threat".

(b) Information Disorder: Toward an interdisciplinary framework for research and policy making, Council of Europe report DGI(2017)09

73. The authors of this report identified three different types of information disorder: misinformation, disinformation and mal-information. Using the dimensions of harm and falseness, they described the differences between these three types as follows:

1. misinformation is when false information is shared, but no harm is meant;
2. disinformation is when false information is knowingly shared to cause harm; and
3. mal-information is when genuine information is shared to cause harm, often by moving information designed to stay private into the public sphere.

74. As the report explains, the "agent" who created a fabricated message might be different to the agent who produced that message, who might also be different from the agent who distributed it. A thorough understanding was needed of who these agents were and what motivated them. There was also a need to examine how mis-, dis- and mal-information were being consumed, interpreted and acted upon – in particular, whether they were being re-shared as the original agent intended, and whether they were continuing to travel online, or if they had moved offline into personal conversations, which were difficult to capture.

75. In the specific context of elections, the report said the following:

"The shock of the Brexit referendum, the US election, Le Pen reaching the run-off vote in the French election and the overturning of the Kenyan election have been used as examples of the potential power of systematic dis-information campaigns. However, empirical data about the exact influence of such campaigns does not exist.

As Danah Boyd argues about recent responses to fears about mis- and dis-information, 'It's part of a long and complicated history, and it sheds light on a variety of social, economic, cultural, technological, and political dynamics that will not be addressed through simplistic solutions.' Certainly, we have to look for explanations for how societies, particularly in the West, have become so segregated in terms of terms of age, race, religion, class and politics. Recognizing the impact of factors such as the collapse of the welfare state, the failure of democratic institutions to provide public services, climate change and miscalculated foreign interventions [is] required. We cannot see the phenomenon of mis- and dis-information in isolation, but must consider its impact amid the new-media ecosystem. This ecosystem is dominated by increasingly partisan radio, television and social media; exaggerated emotional articulations of the world; quick delivery via algorithmically derived feeds on smartphones and audiences that skim headlines to cope with the floods of information before them. Making sense of mis-, dis- and mal-information as a type of information disorder, and learning how it works, is a necessity for open democracies. Likewise, neglecting to understand the structural reasons for its effectiveness is a grave mistake.

...

Fabricated 'news' websites created solely for profit have existed for years. ... However, the US election shone a light on how many of these sites are located overseas, but aimed at US audiences. *Buzzfeed* was one of the first news organisations to detail the phenomenon of English-language websites created by Macedonians to capitalise on US readers' enthusiasm for sensationalist stories. The small city of Veles in Macedonia produced 'an enterprise of cool, pure amorality, free not only of ideology but of any concern or feeling about the substance of the election. These Macedonians on Facebook didn't care if Trump won or lost the White House. They only wanted pocket money to pay for things.'

This example from Veles also underscores the difficulty of assessing the true motivation of any particular agent. The dominant narrative has been that these young people were motivated by the financial benefits. We can assume this is true, as they undoubtedly made money, but we will unlikely ever know whether there was any coordinated attempt to encourage these teenagers to start this type of work in the first place."

76. The report made thirty-four recommendations, targeted at technology companies, national governments, media organisations, civil society, education ministries and funding bodies. In respect of national governments, its recommendations were as follows:

"1. **Commission research to map information disorder**. National governments should commission research studies to examine information disorder within their respective countries, using the conceptual map provided in this report. What types of information disorder are most common? Which platforms are the primary vehicles for dissemination? What research has been carried out that examines audience responses to this type of content in specific countries? The methodology should be consistent across these research studies exercises, so that different countries can be accurately compared.

2. **Regulate ad networks**. While the platforms are taking steps to prevent fabricated 'news' sites from making money, other networks are stepping in to fill the gap. States should draft regulations to prevent any advertising from appearing on these sites.
3. **Require transparency around Facebook ads**. There is currently no oversight in terms of who purchases ads on Facebook, what ads they purchase and which users are targeted. National governments should demand transparency about these ads so that ad purchasers and Facebook can be held accountable.
4. **Support public service media organisations and local news outlets**. The financial strains placed on news organisations in recent years has led to 'news deserts' in certain areas. If we are serious about reducing the impact of information disorder, supporting quality journalism initiatives at the local, regional and national level needs to be a priority.
5. **Roll out advanced cyber-security training**. Many government institutions use bespoke computer systems that are incredibly easy to hack, enabling the theft of data and the generation of mal-information. Training should be available at all levels of government to ensure everyone understands digital security best practices and to prevent attempts at hacking and phishing.
6. **Enforce minimum levels of public service news on to the platforms**. Encourage platforms to work with independent public media organisations to integrate quality news and analysis into users' feeds."

(c) Council of Europe: Disinformation and Electoral Campaigns (June 2019)

77. This report provided an overview of the legal framework in a number of different States. In respect of the United Kingdom, it said the following:

"United Kingdom

The British Electoral Commission has called for increasing transparency for voters with regard to the practice of digital electoral campaigns. It has provided recommendations on the responsibility of digital campaigns, spending on digital campaigns, the transparency of payments for digital campaigns and enforcement of these rules."

78. The report noted that many countries clearly were aware of the dangers of the manipulation of public opinion during electoral campaigns and comprehensive efforts were being made to implement new regulations to counter disinformation. However, there remained many obstacles to drafting effective rules that were compatible with constitutional and international standards.

79. The report made a number of recommendations falling into three categories:

1. digital law regulations which would require transparency from service providers about their activities and the protection of personal data;
2. electoral law regulations, including longer electoral campaigns, transparency of financial resources of providers and a ban on electoral expenditure on digital activities by a foreign legal or physical person; and
3. good practice, including measures which would concentrate on fact-checking, cooperation with all stakeholders, ethics, the development of literacy programmes and the self-regulation of service providers, all supporting quality journalism.

(d) Venice Commission: Urgent Report on the Cancellation of Election Results by Constitutional Courts

80. In this report, issued on 27 January 2025, the Venice Commission responded to a request by the President of the Parliamentary Assembly of the Council of Europe for an urgent report on the following question:
"Under which conditions and under which legal standards can a constitutional court invalidate elections, drawing from the recent Romanian case?"
81. The request followed the annulment by the Romanian Constitutional Court on 6 December 2024 of the first round of the Presidential election, on the basis that information from Romania's intelligence agencies had revealed voter manipulation and distortion of equal opportunities for electoral competitors through the non-transparent use of digital technologies and artificial intelligence in the electoral campaign, as well as through the financing of the electoral campaign from undeclared sources, including online.
82. The Venice Commission took the view that "external influence" – by non-governmental organisations, the media (social media in particular), especially those sponsored and financed from abroad, and foreign State and non-State actors – was not less detrimental and could have the same (or even more severe) consequences as a breach of election rules by candidates, political parties and State officials. However, even though irregularities linked to the registration and campaign parts of the electoral cycle could tilt the playing field in favour of specific candidates and/or have a profound impact on the opinion of voters, it could be more challenging to establish objectively their impact on the election result than it was to establish the impact of irregularities during the voting and counting process.
83. With regard to the new challenges posed by online campaigning and disinformation, the Venice Commission said the following:
"Compared to traditional broadcast and print media, social media flow freely across borders, and in most countries social media and campaigning online are not regulated in the context of elections to the extent that traditional media and traditional campaigning are. Yet the liberal character of social media does not mean that it is beyond national regulation and enforcement in the context of elections. The increasing importance of online campaigning– including by use of AI, which has the potential to magnify the effect of disinformation and manipulation of public opinion – raises new challenges in relation to 1) campaign propaganda, disinformation and the content of campaign messaging; and 2) the rules on campaign finance and transparency, including restrictions on contributions from anonymous and foreign sources, and on misuse of administrative resources. From a legal point of view, it is important to distinguish between these two matters.
As concerns, firstly, campaign propaganda, it should be noted that electoral campaigns are in essence information campaigns by the candidates designed to convince the voters. Statements on policy made by candidates in the context of an election may often be regarded by their opponents as disinformation or false information. Regardless of form and medium, political statements in the context of campaigning are typically value judgments or statements that fall under the candidate's freedom of expression, unless they exceed permissible limits, e.g. in the form of hate speech against political opponents. Considering the ECtHR's jurisprudence on judicial interference with campaign messaging, it is currently hard to see how the form and content of campaign messaging of candidates could amount to a violation of electoral law that may lead to the annulment of the elections.

Ideally, States should regulate the consequences of information disorders, cyber-attacks and other digital threats to electoral integrity. ...

In this connection, attention is drawn to the recent Interpretative declaration of the Code of good practice in electoral matters as concerns digital technologies and artificial intelligence, in which the Venice Commission emphasised 1) that the freedom of voters to form an opinion includes the right to have access to all kinds of information enabling them to be correctly informed before making a decision (which can be affected by online information disorders); and 2) that equality of opportunity also applies to the use of digital technologies and artificial intelligence in the electoral campaign, including the functions and services of internet intermediaries. ...

Secondly, whilst online campaigning based on social media platforms may be novel in form and impact, in the opinion of the Venice Commission its use should still be subject to the general rules on campaign finance and transparency. ...

One challenge in respect of social media, where content is generated by users, is how to attribute online support for a candidate to the campaign of that candidate. The simple fact that a candidate is successful in online campaigning, and that the use of social media platforms may amplify a candidate's message beyond what was possible with print and broadcast media, does not mean that the candidate has violated rules on campaign spending and transparency and thus obtained an unfair advantage. ...

In this connection, attention is drawn again to the Interpretative declaration of the Code of good practice in electoral matters as concerns digital technologies and artificial intelligence, in which the Venice Commission calls on States to regulate, *inter alia*, that online electoral advertising must always be identified as such and must be transparent regarding the identity of its sponsor and the dissemination technique being used; that funding of online activities must be transparent, with potential limits on political parties' spending on digital advertising; and that social media platforms are required to consistently disclose data on political advertising and their sponsors. According to the Interpretative declaration, banning certain forms of paid political advertising on social media during electoral periods may be an option, particularly when automated mass dissemination or micro-targeting techniques based on artificial intelligence are being employed, and the option to prohibit political parties and candidates from campaigning anonymously could also be justified. Furthermore, the Venice Commission has previously stated that third parties should be free to fundraise and express views on political issues as a means of free expression, and their activity should not be unconditionally prohibited; at the same time, some forms of regulation, with comparable obligations and restrictions as apply to parties and party candidates, should be extended to third parties that are involved in the campaign, to ensure transparency and accountability.

As mentioned above in the chapter on procedural questions, procedural safeguards for election disputes gain particular importance when it comes to decisions on cancellation of election results. The law must guarantee safeguards such as impartiality, precise norms to limit the discretion of the authority, guarantees of a fair, objective and reasoned decision, in order to prevent arbitrary decisions and to be in accordance with the ECHR. Proving violations of the law by campaigning online and via social media is particularly challenging. Well-reasoned, transparent decisions on such matters are crucial. In the opinion of the Venice Commission, such decisions should precisely indicate the violations and the evidence, and they must not be based solely on classified intelligence

(which may only be used as contextual information), as this would not guarantee the necessary transparency and verifiability."

III. EUROPEAN UNION

A. Council Regulation (EU) 2022/350 of 1 March 2022 amending Regulation (EU) No 833/2014 concerning restrictive measures in view of Russia's actions destabilising the situation in Ukraine, and Council Decision (CFSP) 2022/351 of 1 March 2022 amending Decision 2014/512/CFSP concerning restrictive measures in view of Russia's actions destabilising the situation in Ukraine

84. The above-mentioned Regulation and Decision underlined the need to further strengthen the resilience of the European Union and Member States as well as their ability to counter hybrid threats, including disinformation and influence operations. Both noted in paragraph (6) of their respective Preambles that

"[t]he Russian Federation has engaged in a systematic, international campaign of media manipulation and distortion of facts in order to enhance its strategy of destabilisation of its neighbouring countries and of the Union and its Member States. In particular, the propaganda has repeatedly and consistently targeted European political parties, especially during election periods, as well as targeting civil society, asylum seekers, Russian ethnic minorities, gender minorities, and the functioning of democratic institutions in the Union and its Member States."

85. Through this Regulation and Decision the European Union prohibited operators from broadcasting any content by certain identified legal persons, entities or bodies, including through transmission or distribution by any means such as cable, satellite, IP-TV, internet service providers, internet video-sharing platforms or applications, whether new or pre-installed. The identified legal persons, entities or bodies were RT- Russia Today English, RT- Russia Today UK, RT- Russia Today Germany, RT- Russia Today France, RT- Russia Today Spanish and Sputnik. A challenge to this Regulation and Decision on the grounds, *inter alia*, that it breached RT's "rights of the defence, freedom of expression and information, freedom to conduct a business and the principle of non-discrimination on grounds of nationality" was rejected by the Grand Chamber of the EU General Court in its judgment of 27 July 2022 in Case T-125/22 *RT France v Council of the European Union* (ECLI:EU:T:2022:483). An appeal to the CJEU (Case C-620/22 P) was withdrawn by RT France on 6 June 2023.

B. The Digital Services Act

86. Under Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act) ("DSA"), designated services with more than 45 million active users ("Very Large Online Platforms" and "Very Large Online Search Engines") in the European Union have the obligation to assess in depth the systemic risks stemming from the design, functioning and use of their services, as well as from potential misuses by the recipients of the service, and should take appropriate measures to mitigate the actual or foreseeable negative effects on democratic processes, civic discourse and electoral processes, as well as public security.

87. When assessing such systemic risks, providers of Very Large Online Platforms and of Very Large Online Search Engines should focus on the systems or other elements that might contribute to the risks, including all the algorithmic systems that might be relevant, in particular their recommender

systems and advertising systems, paying attention to the related data collection and use practices. They should also assess whether their terms and conditions and the enforcement thereof were appropriate, as well as their content moderation processes, technical tools and allocated resources. Such providers should pay particular attention to how their services were being used to disseminate or amplify misleading or deceptive content, including disinformation. Where the algorithmic amplification of information contributed to the systemic risks, those providers should duly reflect this in their risk assessments. Where risks were localised or there were linguistic differences, those providers should also account for this in their risk assessments. Providers of Very Large Online Platforms and of Very Large Online Search Engines should, in particular, assess how the design and functioning of their service, as well as the intentional and coordinated manipulation and use of their services, or the systemic infringement of their terms of service, contributed to such risks. Such risks might arise, for example, through the inauthentic use of the service, such as the creation of fake accounts, the use of bots or deceptive use of a service, and other automated or partially automated behaviours, which might lead to the rapid and widespread dissemination to the public of information that was illegal content or incompatible with an online platform's or online search engine's terms and conditions and that contributed to disinformation campaigns.

C. The European Commission

88. The European Commission recognised that disinformation and foreign information manipulation and interference were a serious threat to societies.[1] They could undermine democratic institutions and processes (such as elections) by preventing people from making informed decisions or discouraging them from voting, and they could polarise societies by pitting communities against each other. As new technologies made it possible for hostile actors to spread disinformation and to manipulate information at a scale and with a speed never seen before, the European Commission indicated that tackling disinformation and information manipulation was one of the most pressing issues for the European Union and its Member States.

89. Consequently, the Commission was strengthening its strategic communication in response to disinformation, foreign information manipulation and interference targeting EU policies. The Commission's response to disinformation was centred around: developing policies to strengthen European democracies, making it more difficult for disinformation actors to misuse online platforms, and protecting journalists and media pluralism; countering foreign interference and cyberattacks through awareness-raising projects, advanced technological solutions, and improved coordination; building societal resilience against disinformation through media literacy and awareness raising; and cooperating with institutions, national authorities, civil society and other organisations.

90. On 26 March 2024 the Commission published guidelines on recommended measures to Very Large Online Platforms and Search Engines to mitigate systemic risks online that might impact the integrity of elections, with specific guidance for the European Parliament elections in June 2024.

91. These guidelines recommended mitigation measures and best practices to be undertaken by Very Large Online Platforms and Search Engines before, during, and after electoral events, such as to:

1. reinforce their internal processes, including by setting up internal teams with adequate resources, using available analysis and information on local context-specific risks and on the

use of their services by users to search and obtain information before, during and after elections, to improve their mitigation measures;

2. implement elections-specific risk mitigation measures tailored to each individual electoral period and local context. Among the mitigation measures included in the guidelines, Very Large Online Platforms and Search Engines should promote official information on electoral processes, implement media literacy initiatives, and adapt their recommender systems to empower users and reduce the monetisation and virality of content that threatened the integrity of electoral processes. Moreover, political advertising should be clearly labelled as such, in anticipation of the new regulation on the transparency and targeting of political advertising;
3. adopt specific mitigation measures linked to generative Artificial Intelligence ("AI"): Very Large Online Platforms and Search Engines whose services could be used to create and/or disseminate generative AI content should assess and mitigate specific risks linked to AI, for example by clearly labelling content generated by AI (such as deepfakes), adapting their terms and conditions accordingly and enforcing them adequately;
4. cooperate with EU level and national authorities, independent experts, and civil society organisations to foster an efficient exchange of information before, during and after the election and facilitate the use of adequate mitigation measures, including in the areas of Foreign Information Manipulation and Interference, disinformation and cybersecurity;
5. adopt specific measures, including an incident response mechanism, during an electoral period to reduce the impact of incidents that could have a significant effect on the election outcome or turnout; and
6. assess the effectiveness of the measures through post-election reviews. Very Large Online Platforms and Search Engines should publish a non-confidential version of such post-election review documents, providing opportunity for public feedback on the risk mitigation measures put in place.

IV. OTHER MATERIALS

The report by the United States' Senate Select Committee on Intelligence

92. Following allegations of interference by Russia in the 2016 Presidential election, a bipartisan report was prepared by the Senate Select Committee on Intelligence. From 2017 to 2019, the Committee held hearings, conducted interviews, and reviewed intelligence related to Russian attempts in 2016 to access election infrastructure. It sought to determine the extent of Russian activities, identify the response of the U.S. Government at the state, local, and federal level to the threat, and make recommendations on how to better prepare for such threats in the future.

93. The Committee completed its report on 8 May 2018 and released an unclassified summary (later followed by the redacted report). The Committee concluded that in 2016 cyber actors affiliated with the Russian Government had conducted an unprecedented, coordinated cyber campaign against state election infrastructure. Russian actors had scanned databases for vulnerabilities, attempted intrusions, and in a small number of cases successfully penetrated a voter registration database. This activity was part of a larger campaign to prepare to undermine confidence in the voting process. However, the Committee had not seen any evidence that vote tallies were manipulated or that voter registration information was deleted or modified.

94. The Committee further found that in addition to cyber activity directed at state election infrastructure, Russia had undertaken a wide variety of intelligence-related activities targeting the U.S. voting process. These activities began at least as early as 2014, continued through Election Day 2016, and included traditional information gathering efforts as well as operations likely aimed at preparing to discredit the integrity of the U.S. voting process and election results.

95. While the full scope of Russian activity against the states remained unclear because of collection gaps, the Committee found ample evidence to conclude that the Russian government was developing capabilities to undermine confidence in the country's election infrastructure, including voter processes.

96. The Committee further found that the initial response of the Department of Homeland Security had been inadequate to counter the threat.

97. Despite the progress on communication and improvements to the security of the election process, the Committee remained concerned about a number of potential vulnerabilities in election infrastructure. In particular, voting systems across the U.S. were outdated, and many aspects of election infrastructure systems were connected to and could be accessed over the Internet.

98. The Senate Select Committee on Intelligence recommended the following steps to better defend against a hostile nation-State which might seek to undermine U.S. democracy: reinforce states' primacy in running elections; create effective deterrence; improve information sharing on threats; secure election-related systems; take steps to secure the vote itself; and provide assistance for the states.

THE LAW

99. The applicants complain under Article 3 of Protocol No. 1 to the Convention that the respondent State breached its positive obligation to investigate hostile State interference in its democratic elections, and that it failed to put in place an effective legal and institutional framework to secure its obligations under that Article.

Article 3 of Protocol No. 1 reads as follows:

"The High Contracting Parties undertake to hold free elections at reasonable intervals by secret ballot, under conditions which will ensure the free expression of the opinion of the people in the choice of the legislature."

I. ADMISSIBILITY

A. The applicability of Article 3 of Protocol No. 1

1. The parties' submissions

(a) The Government

100. The Government argued that the Court had thus far interpreted Article 3 of Protocol No. 1 as imposing a relatively narrow range of obligations on States. The violations found by the Court had generally fallen into one of three broad categories: direct restrictions by the State on who might stand or vote in an election; failure by the State to act in accordance with its own electoral law; and failure by the State to provide a reasonably fair and effective system of remedies for alleged breaches of electoral law. Moreover, this was an area in which the Court had found the margin of appreciation to be wide, as there were numerous ways of organising and running electoral systems and a wealth of differences in, *inter alia*, historical development, cultural diversity and political thought within Europe which it was for each Contracting State to mould into its own democratic vision (the

Government cited, in this respect, *Hirst v. the United Kingdom (no. 2)* [GC], no. 74025/01, § 60, ECHR 2005-IX).

101. According to the Government, the applicants, in seeking to impose on Contracting States obligations to take prescriptive and specific steps to protect people from interference by external third parties, which was said to take the form of spreading incorrect information on social media, and to investigate alleged interferences, were inviting the Court to create a new, prescriptive and far-reaching category of positive obligations under Article 3 of Protocol No. 1 to the Convention. Such duties would significantly extend the recognised obligations on the State in a way which was disconsonant with the Court's principled case-law, and inconsistent with the wide margin of appreciation afforded to States in this area.

102. The Government further argued that there was no authority for the proposition that a procedural obligation to investigate arguable violations of Article 3 of Protocol No. 1 existed. Investigative obligations were rightly described as "adjectival" because they existed to ensure that the primary right was effective (the Government cited, in this respect, *Al Nashiri v. Romania*, no. 33234/12, § 629, 31 May 2018). Since the State was not under any of the positive systemic obligations contended for by the applicants, it could not have been under any duty to investigate arguable breaches of those obligations. Moreover, such a duty would be inconsistent with the wide margin of appreciation enjoyed by States in implementing and securing the rights under Article 3 of Protocol No. 1.

103. There were also serious principled objections to a legal duty being placed on the State to investigate supposed interferences with an election which were not said to have broken domestic electoral law and which had not been shown to have altered the outcome of an election. Such a duty would risk engaging State bodies in an exercise which could be perceived as serving politically partisan ends. It could also engage the courts in a highly politicised and contested context, and would risk exactly the kind of arbitrariness that Article 3 of Protocol No. 1 protected against.

104. Were such a duty to exist, the Government argued that the threshold for its engagement would necessarily be a high one. The core principle of Article 3 of Protocol No. 1 was that the practical effectiveness of the right to vote and stand for election should not be thwarted and its very essence should not be impaired. That threshold had plainly not been met in the present case, even if the applicants' case were to be taken at its highest. There was no suggestion that anyone who wished to vote in an election was prevented from doing so; that any person's vote was not counted; that any voter was intimidated; or that the outcome of any election would or even might have been different as a result of Russian interference. Insofar as the applicants relied on Russia's use of a highly sophisticated network of "bots", "trolls" and other partisan social media and news media sites, it was not clear how these could impair the practical effectiveness of the right of any voter to vote and thereby freely express his or her opinion. Every voter would cast his or her vote for a complex variety of reasons. It was therefore inherently unlikely that any particular piece of incorrect information read online would cause an individual voter to cast his or her vote differently.

(b) The applicants

105. The applicants submitted that Article 3 of Protocol No. 1 imposed an obligation on Contracting States to hold free and fair elections under conditions which would ensure the free expression of the people in the choice of legislature. This encompassed a positive obligation to take active steps to

organise elections under fair conditions (they cited, for example, *Yumak and Sadak v. Turkey* [GC], no. 10226/03, § 106, ECHR 2008), and required the State to ensure that any interference with or limitation to the rights guaranteed by Article 3 of Protocol No. 1 did not thwart the free expression of the people in the choice of legislature (ibid, § 109). The positive obligations in Article 3 of Protocol No. 1 were necessarily context specific, and included guaranteeing pluralism and the absence of compulsion or pressure (see *Yumak and Sadak*, cited above, §§ 106-108, and *Communist Party of Russia and Others v. Russia*, no. 29400/05, §§ 124-126, 19 June 2012), tackling threats to the fairness of the electoral process (see *The Georgian Labour Party v. Georgia*, no. 9103/04, §§ 82-87, ECHR 2008), and establishing a system for the effective investigation of complaints and appeals in electoral matters (see *Namat Aliyev v. Azerbaijan*, no. 18705/06, § 81, 8 April 2010).

106. The applicants pointed out that the Court had already found Article 3 of Protocol No. 1 to entail a positive obligation to ensure that electoral integrity was not undermined by improper domestic pressure (see, for example, *Karimov v. Azerbaijan*, no. 12535/06, §§ 42-50, 25 September 2014; *Namat Aliyev*, cited above, §§ 70-90; and *Communist Party of Russia*, cited above, §§ 107-129). It had specifically (if indirectly) adverted to the risks of direct, malicious interference in elections, and the need to safeguard against this (see *Communist Party of Russia*, cited above, § 123), and confirmed that electoral interference having an "undue influence on voter choice" was an irregularity of a type which could thwart the democratic nature of an election (see *Gahramanli and Others v. Azerbaijan*, no. 36503/11, § 73, 8 October 2015). In their view, as there was no principled difference between threats emanating from the domestic sphere (even from the State itself) and threats emanating from abroad, Article 3 of Protocol No. 1 also had to include a positive obligation to protect an electoral system from external pressure, interference or attacks by foreign actors. The acknowledgement of such an obligation would not expand the scope of the primary right under Article 3 of Protocol No. 1.

107. In the applicants' view, the Government were therefore wrong to suggest that the obligations under Article 3 of Protocol No. 1 were principally negative, and that the only positive duty under that Article was to have in place a reasonably effective independent system of remedies for breaches of electoral law (see the Government's submissions summarised in paragraphs 100 above). In this regard, it was noteworthy that when the Grand Chamber considered the duty to have in place a system of remedies it described it as "an important device at the State's disposal in achieving the fulfilment of its positive duty" under Article 3 of Protocol No. 1 (see *Mugemangango v. Belgium* [GC], no. 310/15, § 69, 10 July 2020).

108. According to the applicants, a necessary corollary of the State's overarching obligation to organise democratic elections under conditions which would ensure the free expression of the opinion of the people in the choice of the legislature was a duty to investigate credible allegations of electoral irregularities or interferences which threatened to undermine the integrity and effectiveness of an electoral procedure aimed at identifying the will of the people through universal suffrage. The State could not properly determine which positive measures to adopt to ensure that the free expression of the opinion of the people was respected if it had failed to investigate or had turned a blind eye to credible allegations of interferences which threatened to undermine that fundamental principle.

109. Consequently, the applicants argued that when faced with credible evidence of improper interference in an election, the State was obliged to take additional steps to obtain more information and verify the accuracy of the allegations (see *Namat Aliyev*, cited above, § 88). The Court had previously identified a requirement to investigate the circumstances leading to the breach of a positive obligation in order to avoid repetition (see, for example, *Mocanu and Others v. Romania* [GC], nos. 10865/09 and 2 others, §§ 317-318, ECHR 2014 (extracts), and *McCann and Others v. the United Kingdom*, 27 September 1995, §§ 146 and 161, Series A no. 324) and the same reasoning underpinned and informed the positive obligation to investigate in the context of Article 3 of Protocol No. 1: the investigation had to ensure, as far as possible, that the full facts were identified so that lessons could be learned and implemented. Such an obligation was necessary for the right in Article 3 of Protocol No. 1 to be practical and effective and neither impinged on the Contracting States' wide margin of appreciation nor interfered with their broad latitude in moulding their own democratic vision.

110. Furthermore, the applicants argued that the contention that an investigatory obligation would engage the courts in a highly politicised and contested context (see the Government's submissions summarised in paragraph 103 above) was no answer to their claim, since all claims of violations of Article 3 of Protocol No. 1 occurred in such a context.

111. As for whether the investigatory obligation was triggered in the present case, the applicants argued that the Government could not rely on the absence of evidence that Russian interference had altered the outcome of an election in a case where the very subject matter of the complaint was that the Government had failed to investigate that issue. It was sufficient that there was evidence that interference had occurred.

2. The Court's assessment

(a) General principles

(i) Democracy and its protection in the Convention system

112. Democracy constitutes a fundamental element of the "European public order". That is apparent, firstly, from the Preamble to the Convention, which establishes a very clear connection between the Convention and democracy by stating that the maintenance and further realisation of human rights and fundamental freedoms are best ensured on the one hand by an effective political democracy and on the other by a common understanding and observance of human rights. The Preamble goes on to affirm that European countries have a common heritage of political traditions, ideals, freedom and the rule of law. This common heritage consists in the underlying values of the Convention; thus, the Court has pointed out on many occasions that the Convention was in fact designed to maintain and promote the ideals and values of a democratic society. In other words, democracy is the only political model contemplated by the Convention and, accordingly, the only one compatible with it (see, among many authorities, *Ždanoka v. Latvia* [GC], no. 58278/00, § 98, ECHR 2006-IV and *United Communist Party of Turkey and Others v. Turkey*, 30 January 1998, § 45, Reports of Judgments and Decisions 1998-I).

113. The rights guaranteed under Article 3 of Protocol No. 1 are crucial to establishing and maintaining the foundations of an effective and meaningful democracy governed by the rule of law and are accordingly of prime importance in the Convention system (see, among other authorities, *Mathieu-Mohin and Clerfayt v. Belgium*, 2 March 1987, § 47, Series A no. 113; *Ždanoka*, cited above, §§ 98 and 103; *Sitaropoulos and Giakoumopoulos v. Greece* [GC], no. 42202/07, § 63, ECHR

2012; *Karácsony and Others v. Hungary* [GC], nos. 42461/13 and 44357/13, § 141, 17 May 2016; *Mugemangango*, cited above, § 67; and *Selahattin Demirtaş v. Turkey (no. 2)* [GC], no. 14305/17, § 382, 22 December 2020). Free elections and freedom of expression, in particular freedom of political debate, form the foundation of any democracy (see *Selahattin Demirtaş (no. 2)*, cited above, § 383, and *Tănase v. Moldova* [GC], no. 7/08, § 154, ECHR 2010).

114. It cannot be ruled out that a person or a group of persons will rely on the rights enshrined in the Convention or its Protocols in order to attempt to derive therefrom the right to conduct what amounts in practice to activities intended to destroy the rights or freedoms set forth in the Convention. It was precisely this concern which led the authors of the Convention to introduce Article 17 (see *Ždanoka*, cited above, § 99; see also *Refah Partisi (the Welfare Party) and Others v. Turkey* [GC], nos. 41340/98, 41342/98, 41343/98 and 41344/98, § 99, ECHR 2003-II). Consequently, in order to guarantee the stability and effectiveness of a democratic system, the State may be required to take specific measures to protect itself. Thus, in *Vogt v. Germany* (26 September 1995, §§ 51 and 59, Series A no. 323), with regard to the requirement of political loyalty imposed on civil servants, the Court acknowledged the legitimacy of the concept of a "democracy capable of defending itself".

115. The Court has also found that pluralism and democracy are based on a compromise that requires various concessions by individuals, who must sometimes be prepared to limit some of their freedoms so as to ensure the greater stability of the country as a whole (see *Ždanoka*, cited above, § 100, and *Refah Partisi (the Welfare Party) and Others*, cited above, § 99). The problem which is then posed is that of achieving a compromise between the requirements of defending democratic society on the one hand and protecting individual rights on the other (see *Ždanoka*, cited above, § 100 and *United Communist Party of Turkey and Others*, cited above, § 32). Every time a State intends to rely on the principle of "a democracy capable of defending itself" in order to justify interference with individual rights, it must carefully evaluate the scope and consequences of the measure under consideration, to ensure that a balance is achieved between the requirements of defending democratic society and protecting individual rights (see *Ždanoka*, cited above, § 100).

116. Finally, with regard to the implementation of measures intended to defend democratic values, the Court stated in *Refah Partisi (the Welfare Party) and Others* (cited above, § 102):

"The Court considers that a State cannot be required to wait, before intervening, until a political party has seized power and begun to take concrete steps to implement a policy incompatible with the standards of the Convention and democracy, even though the danger of that policy for democracy is sufficiently established and imminent. The Court accepts that where the presence of such a danger has been established by the national courts, after detailed scrutiny subjected to rigorous European supervision, a State may 'reasonably forestall the execution of such a policy, which is incompatible with the Convention's provisions, before an attempt is made to implement it through concrete steps that might prejudice civil peace and the country's democratic regime'. ..."

(ii) Article 3 of Protocol No. 1

117. Although Article 3 of Protocol No. 1 differs from the other rights guaranteed in the Convention and its Protocols, as it is phrased in terms of the obligation for the High Contracting Party to hold elections under conditions which ensure the free expression of the opinion of the people rather than in terms of a particular right or freedom, the Court, having regard to the preparatory work on Article 3 of Protocol No. 1 and the interpretation of that provision in the context of the Convention as a

whole, has established that it implies individual rights, primarily the right to vote and to stand for election (see *Selahattin Demirtaş*, cited above, § 385; *Ždanoka*, cited above, § 102; and *Mathieu-Mohin and Clerfayt*, cited above, §§ 46-51).

118. However, since this Article lays down, in general terms, the obligation of the High Contracting Parties to hold free elections by secret ballot "at reasonable intervals, under conditions which ensure the free expression of the opinion of the people", it also guarantees a more general right, namely that of benefiting from legislative elections in accordance with the above-mentioned formula (see *Partija "Jaunie Demokrāti" and Partija "Mūsu Zeme" v. Latvia* (dec.), nos. 10547/07 and 34049/07, 29 November 2007). The State is therefore under an obligation to adopt positive measures to organise elections "under conditions which will ensure the free expression of the opinion of the people in the choice of the legislature" (see *Communist Party of Russia and Others*, cited above, § 107; see also *Yumak and Sadak*, cited above, § 106).

119. Consequently, the Court has to satisfy itself that the conditions in which applicants' individual electoral rights were exercised did not curtail the rights in question to such an extent as to impair their very essence and deprive them of their effectiveness (see *Abdalov and Others v. Azerbaijan*, nos. 28508/11 and 33773/18, § 91, 11 July 2019; *Namat Aliyev*, see above, § 75; *Scoppola v. Italy (no. 3)* [GC], no. 126/05, § 84, 22 May 2012; and *Riza and Others v. Bulgaria*, nos. 48555/10 and 48377/10, § 142, 13 October 2015). Such conditions must not thwart the free expression of the people in the choice of legislature – in other words, they must reflect, or not run counter to, the concern to maintain the integrity and effectiveness of an electoral procedure aimed at identifying the will of the people through universal suffrage (see *Hirst*, cited above, § 62).

120. There can be no democracy without pluralism (see *Gorzelik and Others v. Poland* [GC], no. 44158/98, §§ 89 et seq., 17 February 2004), which cannot be attained without the adoption of certain positive measures. In the field of audio-visual broadcasting the Court has said that where a State "decide[s] to create a public broadcasting system, ... domestic law and practice must guarantee that the system provides a pluralistic service" (see *Manole and Others v. Moldova*, no. 13936/02, §§ 100-101, ECHR 2009 (extracts)). In the context of elections the duty of the State to adopt some positive measures to secure pluralism of views has also been recognised by the Court (see, for example, *Communist Party of Russia and Others*, cited above, § 125; see also, *mutatis mutandis*, *Informationsverein Lentia and Others v. Austria*, 24 November 1993, § 38, Series A no. 276, and *Russian Conservative Party of Entrepreneurs and Others v. Russia*, nos. 55066/00 and 55638/00, §§ 71-72, 11 January 2007).

121. In this regard, the Court is mindful of the stance taken by the Venice Commission that "equality of opportunity" shall be guaranteed to all parties and candidates alike entailing a neutral attitude by State authorities, in particular with regard to the election campaign and coverage by the media (see *Communist Party of Russia and Others*, cited above, § 108; see also paragraph 83 above).

122. The Court has repeatedly warned against prior restraints on free speech (see, for example, *Communist Party of Russia and Others*, cited above, § 127; see also *The Sunday Times v. the United Kingdom (no. 2)*, 26 November 1991, § 51, Series A no. 217), and stressed that in the sphere of political debate wide limits of criticism are acceptable (see *Communist Party of Russia and Others*, cited above, § 127, and *Lingens v. Austria*, 8 July 1986, §§ 41 and 42, Series A no. 103). In *Bowman v. the United Kingdom* (19 February 1998, § 42, *Reports* 1998-I) the Court emphasised the interrelation

between free elections and freedom of expression, holding that "it is particularly important in the period preceding an election that opinions and information of all kinds are permitted to circulate freely".

123. Article 3 of Protocol No. 1 also requires the existence of a domestic system for the effective examination of individual complaints and appeals in matters concerning electoral rights (see *Mugemangango*, cited above, § 69, *Namat Aliyev*, cited above, § 81, and *Davydov and Others v. Russia*, no. 75947/11, § 274, 30 May 2017). The existence of such a system is one of the essential guarantees of free and fair elections and is an important safeguard against arbitrariness in the electoral process (see *Mugemangango*, cited above, § 69 and *Petkov and Others v. Bulgaria*, nos. 77568/01 and 2 others, § 63, 11 June 2009). Such a system ensures the effective exercise of the rights to vote and to stand for election, maintains general confidence in the State's administration of the electoral process and constitutes an important device at the State's disposal in achieving the fulfilment of its positive duty under Article 3 of Protocol No. 1 to hold democratic elections. Indeed, the State's solemn undertaking under Article 3 of Protocol No. 1 and the individual rights guaranteed by that provision would be illusory if, throughout the electoral process, specific instances indicative of failure to ensure democratic elections were not open to challenge by individuals before a competent domestic body capable of effectively dealing with the matter (see *Mugemangango*, § 69; *Namat Aliyev*, § 81; and *Davydov and Others*, § 274, all cited above).

124. For the examination of appeals to be effective, the decision-making process concerning challenges to election results must be accompanied by adequate and sufficient safeguards ensuring, in particular, that any arbitrariness can be avoided. In particular, the decisions in question must be taken by a body which can provide sufficient guarantees of its impartiality. Similarly, the discretion enjoyed by the body concerned must not be excessive; it must be circumscribed with sufficient precision by the provisions of domestic law. Lastly, the procedure must be such as to guarantee a fair, objective and sufficiently reasoned decision (see *Mugemangango*, cited above, § 70, with further references therein).

125. That being said, Article 3 of Protocol No. 1 was not conceived as a code on electoral matters, designed to regulate all aspects of the electoral process (see *Communist Party of Russia and Others*, cited above, § 108) and the margin of appreciation in this area is, consequently, wide (see, for example, *Mugemangango*, cited above, § 73, and *Hirst*, cited above, § 61, with further references therein). There are numerous ways of organising and running electoral systems and a wealth of differences, *inter alia*, in historical development, cultural diversity and political thought within Europe (see *Mugemangango*, cited above, § 73, and *Hirst*, cited above, § 61; see also *Ždanoka*, cited above, § 103). The States therefore "enjoy considerable latitude to establish rules within their constitutional order governing parliamentary elections and the composition of the parliament, and ... the relevant criteria may vary according to the historical and political factors peculiar to each State" (see *Communist Party of Russia and Others*, cited above, § 108, and *Aziz v. Cyprus*, no. 69949/01, § 28, ECHR 2004-V).

126. Thus, the Court has held that any electoral legislation must be assessed in the light of the political evolution of the country concerned, so that features that would be regarded as unacceptable in the context of one system may be justified in the context of another. It has, however, emphasised that the State's margin of appreciation in this regard is limited by the obligation to respect the

fundamental principle of Article 3 of Protocol No. 1, namely "the free expression of the opinion of the people in the choice of the legislature" (see *Mugemangango*, cited above, § 73; *Mathieu-Mohin and Clerfayt*, cited above, § 54; and *Tănase*, cited above, § 157).

(iii) The procedural obligation to investigate

127. The Court has held that the obligations under Articles 2, 3 and 4 of the Convention, read in conjunction with the State's general duty under Article 1 of the Convention to "secure to everyone within [its] jurisdiction the rights and freedoms defined in [the] Convention", require that there should be some form of effective official investigation when individuals raise an arguable claim that they have suffered treatment infringing those Articles (in the context of Article 2, see, among many examples, *McCann and Others*, cited above, § 161, and *Kaya v. Turkey*, 19 February 1998, § 86, *Reports* 1998-I; in respect of Article 3, see, among many examples, *Assenov and Others v. Bulgaria*, 28 October 1998, § 102, *Reports* 1998-VIII; *El-Masri v. the former Yugoslav Republic of Macedonia* [GC], no. 39630/09, § 182, ECHR 2012; and *X and Others v. Bulgaria* [GC], no. 22457/16, § 184, 2 February 2021; and, in respect of Article 4, see *Rantsev v. Cyprus and Russia*, no. 25965/04, §§ 283 and 288, ECHR 2010 (extracts)), regardless of whether the treatment is imputable to State agents (see *Menson v. the United Kingdom* (dec.), no. 47916/99, ECHR 2003-V; *X and Others v. Bulgaria*, cited above, § 184; and *Rantsev*, cited above, § 289). The investigation is a means of ensuring that the legislative and administrative framework set up to protect the substantive rights is properly implemented and any breaches of that right are repressed and punished (see, for example, *Armani Da Silva v. the United Kingdom* [GC], no. 5878/08, § 230, 30 March 2016 and *Giuliani and Gaggio v. Italy* [GC], no. 23458/02, § 298, ECHR 2011 (extracts)). It should therefore be capable of leading to the identification and punishment of those responsible (see, for example, *El-Masri*, cited above, § 182).

128. While all Convention rights must be interpreted so as to ensure that they are practical and effective, and not theoretical and illusory (see, among many examples, *Selahattin Demirtaş (no. 2)*, cited above, § 386), the Court has been extremely cautious in extending this freestanding procedural obligation to investigate to cases which do not concern alleged breaches of the non-derogable rights in Articles 2, 3 and 4 of the Convention. It has done so in certain Article 8 cases concerning grave interferences with physical or psychological integrity (see, for example, *M.C. v. Bulgaria*, no. 39272/98, § 153, ECHR 2003-XII, which concerned rape; *Mehmet Ulusoy and Others v. Turkey*, no. 54969/09, §§ 90-93, 25 June 2019, which concerned remedies for medical negligence; *Volodina v. Russia (no. 2)*, no. 40419/19, § 49, 14 September 2021, which concerned cyberviolence; and *Petrovic and Others v. Croatia*, nos. 32514/22, 33284/22 and 15910/23, § 147, 14 January 2025, which concerned the abduction of new-born babies from State-run hospitals). In addition, in a small number of Article 1 of Protocol No. 1 cases it has established the need for a criminal investigation in the event of theft or fraud (for example, *Blumberga v. Latvia*, no. 70930/01, §§ 67-68, 14 October 2008; *Nikolay Kostadinov v. Bulgaria*, no. 21743/15, § 55, 8 November 2022; and *Korotyuk v. Ukraine*, no. 74663/17, §§ 36-37, 19 January 2023).

129. However, "the obligation to investigate is less exacting with regard to less serious crimes, such as those involving property, than with regard to more serious ones, such as violent crimes, and in particular those which would fall within the scope of Articles 2 and 3 of the Convention" (see *Blumberga*, cited above, § 67-68). In cases falling under Articles 2, 3 and 4 of the Convention, the effectiveness of the investigation has been assessed by reference to the adequacy of the investigative

measures, the promptness of the investigation, the independence of the investigation and the involvement of the victim (see, for example, *Armani da Silva*, cited above, §§ 232-237 and *El Ma*sri, cited above, §§ 182-185). In the context of less serious crimes "the State will only fail to fulfil its positive obligation ... where flagrant and serious deficiencies in the criminal investigation or prosecution can be identified"; and the possibility of bringing civil proceedings against the alleged perpetrators of a crime might provide the victim with a viable alternative means of securing the protection of his rights, even if criminal proceedings have not been brought to a successful conclusion, provided that the lack of prospects of success of civil proceedings is not "the direct consequence of exceptionally serious and flagrant deficiencies in the conduct of criminal proceedings arising out of the same set of facts" (see *Blumberga*, cited above, § 67-68).

(b) Application of those principles to the facts of the present case

130. As the Government correctly point out (see paragraph 100 above), to date the majority of violations of Article 3 of Protocol No. 1 found by the Court have fallen into one of three broad categories: direct restrictions by the State on who may stand or vote in an election; failure by the State to act in accordance with its own electoral law; and failure by the State to provide a reasonably fair and effective system of remedies for alleged breaches of electoral law. However, the Court has acknowledged that as Article 3 of Protocol No. 1 lays down, in general terms, the obligation of the High Contracting Parties to hold free elections by secret ballot "at reasonable intervals, under conditions which ensure the free expression of the opinion of the people", it also guarantees a more general right, namely that of benefiting from legislative elections in accordance with the above-mentioned formula (see *Partija "Jaunie Demokrāti" and Partija "Mūsu Zeme"*, cited above).

131. Member States are therefore under an obligation to adopt positive measures to organise elections "under conditions which will ensure the free expression of the opinion of the people in the choice of the legislature" (see *Communist Party of Russia and Others*, cited above, § 107; see also *Yumak and Sadak*, cited above, § 106), and there may be a violation of Article 3 of Protocol No. 1 if the conditions in which applicants' individual electoral rights are exercised curtail their rights under that Article to such an extent as to impair their very essence and deprive them of their effectiveness (see the case-law cited in paragraph 119 above). The scope of this obligation extends beyond the integrity of the result of the election, in the narrow sense, and encompasses the circulation of political opinions and information in the period preceding an election (see *Communist Party of Russia and Others*, cited above, § 79; see also, *mutatis mutandis*, *Bowman*, cited above, § 42) and, more generally, the equality of opportunity afforded to candidates (see paragraphs 83 and 121 above).

132. To date, cases falling under this head have concerned conditions created by (or within) the respondent State which, it was argued, thwarted the free expression of the opinion of the people in the choice of legislature. For example, in *Communist Party of Russia and Others* (cited above) the applicants – two political parties and six opposition candidates – complained that their right to free elections guaranteed by Article 3 of Protocol No. 1 to the Convention had been breached on account of the biased media coverage of the 2003 parliamentary elections campaign by the major television stations. Although Russian law guaranteed the neutrality of the broadcasting companies, the applicants claimed that the law was not complied with in practice, and that *de jure* neutrality of the five nationwide channels did not exist *de facto*. The Court found that the respondent State had been under a positive obligation to intervene in order to open up the media to different viewpoints.

However, it considered that the respondent State had taken certain steps to guarantee some visibility of opposition parties and candidates on Russian television. While these arrangements probably did not secure *de facto* equality of all competing political forces in terms of their presence on television screens, having regard to the margin of appreciation enjoyed by the States under Article 3 of Protocol No. 1, it could not be considered established that the State had failed to meet its positive obligations in this area to such an extent that it amounted to a violation of that provision (ibid, §§ 126-128).

133. Nonetheless, although the Court has, to date, only dealt with cases concerning conditions created by (or within) the respondent State which, it was argued, thwarted the free expression of the opinion of the people in the choice of legislature, the object and purpose of the Convention require its provisions to be interpreted and applied in such a way as to make their stipulations not theoretical or illusory but practical and effective (see, among many examples, *Selahattin Demirtaş (no. 2)*, cited above, § 386).

134. In this regard, it is not in dispute that State actors and non-State actors have weaponised disinformation in order to interfere in democratic elections. While new technologies, such as social media platforms, have enabled political parties to disseminate information directly to the electorate, they have also made it possible for hostile actors to spread disinformation and manipulate information at a scale and with a speed never seen before (see paragraphs 64, 67 and 88 above). The NCSC, which is part of one of the United Kingdom Intelligence Agencies, has said that it is "no secret" that Russia seeks to weaken and divide its adversaries by interfering in elections using mis- and disinformation, cyber-attacks and other methods (see paragraph 56 above). In addition, the Council of the European Union has indicated that the Russian Federation has engaged in a systematic, international campaign of media manipulation and distortion of facts in order to enhance its strategy of destabilisation of its neighbouring countries and of the European Union and its Member States (see paragraph 84 above). More specifically, both the United Kingdom and the United States of America have acknowledged that there were attempts by the Russian Federation to interfere in their democratic elections (see paragraphs 53 and 93 above).

135. It is also not in doubt that the dissemination of disinformation is capable of posing a significant threat to democracy. The Office of the UN High Commissioner for Human Rights has acknowledged that widespread disinformation might pose significant threats to the right to stand for elections and vote, and could therefore result in prerequisite rights to free and genuine elections being violated (see paragraph 64 above). The UN Human Rights Council has emphasised that disinformation is a threat to democracy that can suppress political engagement, engender or deepen distrust towards democratic institutions and processes, and hinder the realization of informed participation in political and public affairs (see paragraph 65 above). Moreover, according to the Venice Commission, "a new era of information disorder" has "distorted the communication ecosystem to the point where voters may be seriously encumbered in their decisions by misleading, manipulative and false information designed to influence their votes" (see paragraph 71 above).

136. Accordingly, the Court would accept that if there was a real risk that as a consequence of interference by a hostile State the rights of electors within a member State would be curtailed to such an extent as to impair their very essence, namely the free expression of the opinion of the people in the choice of their legislature, and deprive them of their effectiveness (see the case-law cited in

paragraph 119 above), Article 3 of Protocol No. 1 may require that State to adopt positive measures to protect the integrity of its electoral processes, and to keep those measures under review.

137. The applicants have sought to rely on the Court's Article 2 jurisprudence to support their contention that the State was under a further duty to investigate allegations of interference by Russia in the United Kingdom's electoral processes (see paragraph 109 above). However, there is nothing in the Court's case-law to imply the existence, under Article 3 of Protocol No. 1, of a freestanding procedural obligation to investigate arguable claims of a breach of individuals' rights under that Article (see paragraphs 127-129). Such cases are of a wholly different order from those falling under Articles 2, 3, 4, 8 and even Article 1 of Protocol No. 1, in which the Court has found there to exist a freestanding procedural obligation to investigate. Those cases primarily concerned criminal actions against an individual and/or grave interferences with an individual's physical or psychological integrity. The investigatory obligation was a corollary to the State's positive obligation to protect individuals from breaches of those rights by, *inter alia*, putting in place a regulatory framework for those purposes; in order to secure the effective implementation of that regulatory framework, the State had a separate obligation to investigate arguable claims of breaches of those rights, and the investigation had to be capable of leading to the identification and punishment of the persons responsible.

138. In view of the very different nature of complaints falling under Article 3 of Protocol No. 1, the Court does not consider that a freestanding obligation to investigate, analogous to that which exists where there is an arguable breach of, *inter alia*, Articles 2, 3 and 4 of the Convention, can or should now be read into that Article. At the same time, if a State were to ignore credible allegations of foreign interference in its elections, it would not be in a position to adopt positive measures to protect the integrity of its electoral processes (see paragraph 136 above). Therefore, while States may not have a separate and autonomous obligation to investigate arguable claims of a breach of an individual's rights under Article 3 of Protocol No. 1, a flagrant failure by a State to investigate credible allegations of interference in its elections could raise an issue under that Article if it impeded its ability to take positive measures to protect the electorate from the impairment of the very essence of its right to benefit from elections "under conditions which ensure the free expression of the opinion of the people".

139. The purpose of any investigation would principally be to determine the nature and extent of the threat so as to enable the State to take the measures necessary to protect the integrity of its electoral processes from external interference. The investigation would therefore be antecedent to the State putting in place or updating a legal and regulatory framework to satisfy the positive obligation to protect the integrity of its electoral processes, and any alleged failure to investigate will fall to be considered as part of that positive obligation (see paragraph 136 above), and not as a separate violation of Article 3 of Protocol No. 1.

140. Therefore, to the extent identified in the proceeding paragraphs, the Court considers that Article 3 of Protocol No. 1 is applicable to the applicants' complaints.

B. Victim status

1. The parties' submissions

141. The Government argued that the applicants were not victims, within the meaning of Article 34 of the Convention, of any alleged violation of Article 3 of Protocol No. 1. The present application

was therefore an *action popularis* raising issues which were more appropriately addressed through the democratic institutions of State.

142. The applicants argued that they were "victims" of the alleged violations because, as members of the United Kingdom electorate and sitting members of the legislature, their rights were directly affected by the respondent State's inaction.

2. The Court's assessment

143. In order to be able to lodge a petition by virtue of Article 34, a person, non-governmental organisation or group of individuals must be able to claim to be the victim of a violation of the rights set forth in the Convention. In order to claim to be a victim of a violation, a person must be personally and directly affected by the impugned act or omission (see *Verein KlimaSeniorinnen Schweiz and Others v. Switzerland* [GC], no. 53600/20, § 466, 9 April 2024). The Convention does not envisage the bringing of an *actio popularis* for the interpretation of the rights it contains (see *Tănase*, cited above, § 104), and the Court's task is not normally to review the relevant law and practice *in abstracto*, but rather to determine whether the manner in which they were applied to, or affected, the applicant gave rise to a violation of the Convention (see *Verein KlimaSeniorinnen Schweiz and Others*, cited above, § 460).

144. In principle, anyone eligible to stand for election or vote in a member State could be a potential victim of a failure by that State to adopt positive measures to protect the integrity of its electoral processes. However, as the Court's task is not normally to review the relevant law and practice *in abstracto,* in order to demonstrate "victim status" an applicant would have to produce reasonable and convincing evidence of the likelihood that the right to benefit from elections held "under conditions which ensure the free expression of the opinion of the people" would be curtailed to such an extent as to impair its very essence; mere suspicion or conjecture will be insufficient (see, *mutatis mutandis*, *Verein KlimaSeniorinnen Schweiz and Others*, cited above, § 470; *Communauté genevoise d'action syndicale (CGAS) v. Switzerland* [GC], no. 21881/20, § 108, 27 November 2023; and *Centre for Legal Resources on behalf of Valentin Câmpeanu v. Romania* [GC], no. 47848/08, § 101, ECHR 2014).

145. In order for this test to be met, there must exist evidence of interference of sufficient intensity to be capable of impairing the very essence of the right to benefit from elections held "under conditions which ensure the free expression of the opinion of the people".

146. The applicants in the present case rely on the DCMS and ISC reports (see paragraphs 37-40 and 41-51 above) as evidence of interference by Russia in the United Kingdom's electoral processes, through the spreading of disinformation and the running of "influence campaigns" (encompassing not only the spreading of disinformation but also other tactics such as illicit funding, disruption of electoral mechanics or direct attacks on one of the campaigns, for example using "hack and leak" tactics – see paragraph 44 above). The DCMS and ISC reports, having been prepared prior to the 2019 election, principally focused on interference during the 2016 EU referendum, which was not "an election concerning the choice of the legislature" (see *Moohan and Gillan v. the United Kingdom* (dec.), nos. 22962/15 23345/15, § 42, 13 June 2017). However, it is clear from both reports that Russia posed a significant and ongoing threat to the United Kingdom's democratic processes (see paragraph 43 above) through disinformation campaigns and political influence operations (see paragraph 45 above). This threat was not unique to the United Kingdom; at the time the reports

were published concerns had been raised by the Council of Europe about the threat to democratic elections emanating from influence campaigns by, *inter alia*, hostile State actors (see paragraphs 67-79 above), and there had been a widely-publicised report by the Senate Select Committee on Intelligence into Russian interference in the 2016 US election (see paragraphs 92-98 above). Furthermore, the respondent Government in its response to the ISC report (see paragraphs 52-54 above) acknowledged that it was "almost certain that Russian actors sought to interfere in the 2019 General Election through the online amplification of illicitly acquired and leaked Government documents." The response referred to "several incidents during the 2019 General Election including distributed denial of service attacks against political parties, and suspicious emails received by candidates".

147. As the Court has acknowledged that influence campaigns are capable of posing a significant threat to democracy – notably, by distorting the communication ecosystem to the point where voters might be seriously encumbered in their decisions by misleading, manipulative and false information designed to influence their votes (see paragraph 135 above) – in the present case it would accept that there was evidence of interference in the United Kingdom' democratic processes of sufficient intensity to be capable of impairing the very essence of the right to benefit from elections held "under conditions which ensure the free expression of the opinion of the people".

148. However, the question of whether or not interference is in practice capable of impairing the very essence of the right to benefit from elections held "under conditions which ensure the free expression of the opinion of the people" depends not only on the intensity of the interference but also on the measures in place at the national level to minimise the risk of that interference influencing the outcome of an election. This issue is closely bound up with those which the Court will have to consider when examining the applicants' substantive complaints. It should therefore be joined to the examination on the merits.

C. Other inadmissibility grounds

149. The Court notes that the applicants' complaint is neither manifestly ill-founded nor inadmissible on any other grounds listed in Article 35 of the Convention. It must therefore be declared admissible.

II. MERITS

A. The parties' submissions

1. The applicants

150. While the applicants accepted that the State had a margin of appreciation in how it discharged its duty to have in place an effective legal and institutional framework to secure its obligations under Article 3 of Protocol No. 1, they argued that this margin should not be all-embracing. For example, the margin of appreciation was usually narrow in cases where the State had failed to give any thought to an issue or had failed to act (see *Animal Defenders International v. the United Kingdom* [GC], no. 48876/08, § 116, ECHR 2013 (extracts)). It would be more limited still where, as here, there was a European and international consensus on the standards to be achieved, with which the respondent State was out of step.

151. The applicants further argued that the current domestic legal framework in the United Kingdom failed to satisfy the obligation to have in place an effective framework for the conduct of democratic elections under conditions which ensured the free expression of the opinion of the

people. There was no legal entity with legal responsibility to prevent and combat foreign interference in United Kingdom elections, and the various entities which did have responsibilities in this area were reluctant to acknowledge or use their powers. The existing framework was therefore diffuse and inadequate. Furthermore, the developments that had occurred after the present application was lodged were "too little, too late". They did not address the serious concerns of the ISC (see paragraphs 41-51 above) and they did not discharge the respondent State's positive obligation under Article 3 of Protocol No. 1.

152. Finally, the applicants contended that in the present case objective and credible evidence of Russian interference was set out in the ISC Report (see paragraphs 41-51 above). Notwithstanding the findings made in that report, the respondent Government had failed to conduct an investigation into Russian interference in democratic elections in the United Kingdom. Without such an investigation, there was an unacceptable risk of repetition.

2. The Government

153. According to the Government, the phenomenon of disinformation spread online by hostile foreign States raised complex issues which required careful consideration. There was no uniform answer and no consensus among Contracting States as to what sort of political and legislative responses were appropriate. Furthermore, given the State's obligation to respect and facilitate freedom of expression, particularly in the context of political speech, any requirement on the State to act as referee of public debate should necessarily be limited.

154. The Government therefore argued that in this area the margin of appreciation under Article 3 of Protocol No. 1 was wide. While the Government accepted that there was an international consensus that foreign interference in elections via the Internet, and disinformation generally, was an issue of concern that States should take seriously, there was no international consensus about what should be done about it, or what any domestic legislative response should look like. Nonetheless, it was absurd to suggest – as the applicants did (see paragraph 150 below) – that the Government had given no thought to the issues raised by this case. On the contrary, a range of mechanisms had been put in place, or were being put in place, to tackle the phenomenon of disinformation spread online by hostile foreign States.

155. In this regard, the Government argued that the United Kingdom had in place an effective legal and institutional framework, which was kept under regular review, and it continued to implement and develop policies and legislative proposals to address some of the issues raised by the applicants. For example, the National Security Act 2023 ("NSA 2023" – see paragraphs 25-27 above) contained a Foreign Influence Registration Scheme designed to protect the country from foreign threats, and the Elections Act 2022 ("the 2022 Act" – see paragraph 23 above) implemented controls on online advertising in the context of political campaigns. In addition, specific Government Ministers had responsibility for matters of national security, including addressing the threat of foreign State interference. Other bodies, such as the Electoral Commission, the police and the Security and Intelligence Agencies, had related legal duties and functions.

156. The Government further argued that the intelligence and security Agencies and the police already investigate credible allegations of hostile State activity and potential criminal offences in relation to the holding of elections. Moreover, issues concerning attempted foreign State interference in domestic elections remained under regular consideration by the relevant organs of Government,

and the conduct of investigations, the development of policy and legislative proposals and diplomatic efforts in connection with the prevention of hostile State activities continued to be informed by the work of Parliamentary Committees. Given the sensitivity and security implications of some of these issues, much of the work could not be addressed in the public domain, and in any event could not be the subject of a public inquiry.

3. The third party intervenor

157. In its third party intervention the European Information Society Institute ("EISI") argued that digital advertising was crucial for modern politics and the transparency of how politicians talked to voters was the defining problem of our times. In the pre-election context, it was important that voters were informed about who was speaking to them and why they were being targeted and, in the post-election context, substantiated allegations of election manipulation had to be investigated by impartial bodies. Transparency in both cases helped to solidify public trust in the democratic system.

B. The Court's assessment

158. While the Court does not underestimate the threat posed by the spreading of disinformation and the running of "influence campaigns", their nature is nevertheless such that it is difficult to assess accurately the impact that they may have on individual voters and, by extension, on the outcome of a given election. The ISC report expressly recognised that the impact of Russia's attempts to influence elections in the United Kingdom would be "difficult – if not impossible – to assess" and consequently the ISC did not seek to do it (see paragraph 46 above). Similarly, the Council of Europe report DG1(2017)09 points out that while recent shock election results have been used as examples of the potential power of systemic disinformation campaigns, empirical data about the exact influence of such campaigns does not exist (see paragraph 75 above). More recently, the Venice Commission in its Urgent Report on the Cancellation of Election Results by Constitutional Courts acknowledged that it could be more challenging to establish objectively the impact of external influence campaigns on the election result than it was to establish the impact of irregularities during the voting and counting process (see paragraph 82 above). The Court has itself acknowledged, in the context of a case concerning, *inter alia*, the exceeding by certain parties of the limits on election expenditure, that propaganda carried out by a political party or a candidate in the context of its electoral campaign would not be the only factor motivating the choice of its potential voters. That choice would also be affected by other factors, including those of a political, economic, sociological and psychological nature, with the consequence that it would be very difficult, if not impossible, to determine the exact and real causal link between "excessive" political advertising and the number of votes obtained by the party or candidate in question (see *Partija "Jaunie Demokrāti" and Partija "Mūsu Zeme"*, cited above).

159. The fact that it is difficult to assess the impact of attempts by foreign agents to influence an election should not prevent States from taking measures to defend democratic values; indeed, the Court has made it clear that States are not required to wait, before intervening, until a threat to democracy is sufficiently established and imminent (see the case-law quoted in paragraph 116 above). However, while there is undoubtedly agreement among the international community that election interference through the weaponisation of disinformation and, in some cases, cyber-attacks and "hack and leak" operations, poses a serious threat to democracy, at present there would appear

to be no clear consensus as to what specific actions States would need to take to protect their democratic processes against such risks.

160. In fact, the only area where there appears to be a clear consensus is in the conclusion that this is a complex global problem which cannot be addressed without the co-operation of international partners and social media companies. While warning of the dangers of disinformation and foreign election interference, international organisations have been equally vocal in warning against the risk of kneejerk reactions to these dangers. The impact of disinformation and influence campaigns depends on a variety social, economic, cultural, technological and political dynamics that do not lend themselves to simplistic solutions (see the Council of Europe report DGI(2017)09, quoted in paragraph 75 above). These dynamics need to be properly understood in order for the problem to be addressed effectively. Furthermore, there is a very fine line between addressing the dangers of disinformation and outright censorship. The UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression has criticised responses by States made with "sub-optimal knowledge of online harm, and without adequate data, research or public consultations", which were incompatible with international human rights law and which contributed to amplifying misperception, fear and mistrust of institutions (see paragraph 66 above). In addition, the Office of the UN High Commissioner for Human Rights has advised States to refrain from the general and ambiguous prohibition of the dissemination of information, which could provide the authorities with a broad remit to censor the expression of unpopular, controversial or minority opinions, as well as criticism of the Government in the run up to an election (see paragraph 64 above).

161. Consequently, any actions taken by States to counter the risk of foreign election interference through the dissemination of disinformation and the running of influence campaigns would have to be balanced against the right to freedom of expression under Article 10 of the Convention. In the context of Article 10, the Court has acknowledged that "it is particularly important in the period preceding an election that opinions and information of all kinds are permitted to circulate freely" (see the case-law quoted in paragraph 122 above). While the circulation of disinformation or misinformation could potentially interfere with the right to receive information inherent in Article 10, so could any measures taken to counter its circulation. Therefore, any such measures would need to be calibrated carefully to ensure that they do not interfere disproportionately with individuals' right to impart and receive information, especially in the period preceding an election, and take due account of the risk of abuse by Contracting States seeking to interfere in the outcome of their own elections. Indeed, the Court has previously held that a requirement to label organisations, media outlets and individuals as "foreign agents" violated Articles 10 and 11 of the Convention because the legislative framework and its application were arbitrary and not necessary in a democratic society; and it "contributed to shrinking democratic space by creating an environment of suspicion and mistrust towards civil society actors and independent voices, thereby undermining the very foundations of a democracy" (see *Kobaliya and Others v. Russia*, nos. 39446/16 and 106 others, § 98, 22 October 2024; see also *Ecodefence and Others v. Russia*, nos. 9988/13 and 60 others, 14 June 2022).

162. Therefore, while States should not remain passive when faced with evidence that their democratic processes are under threat (see, *mutatis mutandis*, *Refah Partisi (the Welfare Party) and Others* (cited above, § 102)), they must be accorded a wide margin of appreciation in the choice of

means to be adopted in order to counter such threats. Indeed, in this regard the Court has already held that they "enjoy considerable latitude to establish rules within their constitutional order governing parliamentary elections" (see *Communist Party of Russia and Others*, cited above, § 108, and *Aziz*, cited above, § 28).

163. In the Court's view, the United Kingdom's response to the threat of Russian election interference did not fall outside the wide margin of appreciation afforded to it in this area.

164. There were undoubtedly shortcomings in the Government's initial response. In this regard, the ISC observed that "[t]he written evidence provided to us appeared to suggest that [the Government] had not seen or sought evidence of successful interference in UK democratic processes or any activity that has had a material impact on an election" (see paragraph 48 above). However, despite these initial shortcomings, there were in fact two thorough and independent investigations into Russian interference in the United Kingdom's democratic processes.

165. The first report was by the DCMS, a cross-party committee of MPs appointed by the House of Commons. It conducted an inquiry on disinformation over the course of eighteen months covering, *inter alia*, how individuals' political choices might be affected and influenced by online information and interference by malign forces in political elections in the United Kingdom. Its report was published in February 2019 (see paragraphs 37 and 38 above).

166. The second report was by the ISC, a statutory committee with responsibility for oversight of the United Kingdom Intelligence Community. Its nine Members were drawn from both Houses of Parliament, and appointed by the Houses of Parliament, having been nominated by the Prime Minister in consultation with the Leader of the Opposition. Throughout 2018 the ISC conducted a major Inquiry covering various aspects of the Russian threat to the United Kingdom, together with an examination of how the United Kingdom Government had responded (see paragraphs 41 and 42 above). In its public response to the ISC report, the Government referred to "an ongoing criminal investigation" (see paragraph 54 above), although no further details have been provided about the nature, progress and/or outcome of that investigation.

167. In their application to the Court the applicants have not specified what further measures the respondent Government ought to have taken to investigate allegations of Russian interference in its democratic processes. Before the domestic courts they called for a public inquiry (see paragraph 8 above). However, as the High Court noted, a public inquiry did not have investigatory powers of the type that the police and Intelligence Agencies had and, as a consequence, could not fill any investigatory gap, if it existed (see paragraph 12 above).

168. In any event, following the publication of the ISC report, the Government went on to introduce three new Acts of Parliament: the Elections Act 2022 ("the 2022 Act"), the National Security Act 2023 ("the NSA 2023") and the Online Safety Act 2023 ("the OSA 2023").

169. The 2022 Act restricted third-party election spending to United Kingdom-based entities and eligible overseas electors only, and Part 6 introduced a new requirement for digital campaigning material to display a digital imprint, with the name and address of the promoter of the material or any person on behalf of whom the material was being published (and who was not the promoter – see paragraphs 23-24 above). The NSA 2023 explicitly criminalised assisting a foreign intelligence service in carrying out activities in the United Kingdom where such conduct was prejudicial to the United Kingdom's safety and interests; established a new offence of sabotage designed to capture

State-linked saboteurs who acted in a way that was prejudicial to the United Kingdom's safety; established a new offence of foreign interference; increased the maximum custodial penalties for certain election-related offences that were carried out for or on behalf of, or with the intention to benefit, a foreign power; and introduced a Foreign Influence Registration Scheme (see paragraphs 26-27 above). The OSA 2023 established a new regulatory regime holding tech companies accountable to an independent regulator and addressed misinformation and disinformation where it constituted illegal content or content harmful to children (see paragraph 28 above).

170. In addition to these legislative measures, the Government also created a Counter Disinformation Unit ("the CDU") and the "Defending Democracy" Taskforce. The CDU (now known as the National Security Online Information Team ("NSOIT")) was set up in 2019 and leads the domestic operational and policy response for countering disinformation across Government. It also proactively monitors for harmful narratives that threaten the United Kingdom, and co-ordinates with Government departments to deploy the appropriate response to mis/disinformation (see paragraphs 32-33 above). The "Defending Democracy" Taskforce was launched in 2022 and has the aim of protecting "the democratic integrity of the UK" with "particular focus on foreign interference". It works with local councils, police forces and global tech companies to ensure that electoral processes and infrastructure are secure and resilient, ensure elected officials are protected "at all levels" from physical, cyber, and additional threats, and counter disinformation efforts aimed at "disrupting our national conversation and skewing our democratic processes" (see paragraphs 34-36 above).

171. Furthermore, the need for further measures to counter threats by hostile State actors would appear to be being kept under review, for example by the Independent Reviewer of Terrorism Legislation (see paragraphs 58-61 above).

172. While the applicants have criticised these measures as "too little, too late" (see paragraph 151 above), the measures nevertheless appear to address the points raised by the applicants in their judicial review application (see paragraph 16 above). In any event, any failings cannot be considered to be sufficiently grave as to have impaired the very essence of the applicants' right under Article 3 of Protocol No. 1 to benefit from elections held "under conditions which ensure the free expression of the opinion of the people" (see the case-law cited in paragraphs 119 and 131 above).

173. In the light of the foregoing, the Court concludes that there has been no violation of Article 3 of Protocol No. 1 to the Convention. Consequently, there is no need to decide on the Government's preliminary objection concerning the applicants' victim status (see, for example, *Communist Party of Russia and Others*, cited above, §§ 80 and 129).

FOR THESE REASONS, THE COURT, UNANIMOUSLY,

1. *Decides* to join to the merits the Government's objection concerning the victim status of the applicants;
2. *Declares* the application admissible;
3. *Holds* that there has been no violation of Article 3 of Protocol No. 1 to the Convention, and that it is not necessary to decide on the Government's objection concerning the victim status of the applicants.

Done in English, and notified in writing on 22 July 2025, pursuant to Rule 77 §§ 2 and 3 of the Rules of Court.

Simeon Petrovski
Deputy Registrar

Lado Chanturia
President

In accordance with Article 45 § 2 of the Convention and Rule 74 § 2 of the Rules of Court, the concurring opinion of Judge Jakab is annexed to this judgment.

CONCURRING OPINION OF JUDGE JAKAB

1. While I agree with the outcome of the judgment, I would have preferred a more elaborate analysis of certain general questions. This case concerns the heart of the Court's mission; it is complex, consequential, and extremely timely, yet the relevant standards in the Court's case-law have so far not been sufficiently developed and detailed.

2. The establishment of the Court was part of a peace project after the Second World War. This project has largely been based on the insight that peace in Europe is significantly more likely with liberal democracies, which are built on the principles of democracy and the rule of law, including human rights protection. It is therefore at the very core of the Court's mission to prevent the erosion of liberal democracy.[2] Viewed from this perspective, human rights protection in concrete cases is a legal technique, an institutional proxy to achieve this overarching purpose. In every case, therefore, we should emphatically consider what the direct and indirect effects of the Court's judgment would be on the institutional system of liberal democracy in all Contracting Parties, and we should give preference to those interpretations of the Convention which directly or indirectly strengthen their resilience. If the institutional machinery of liberal democracy erodes, all other potential achievements of human rights protection are likely to slowly fade away as well.

3. Guaranteeing the integrity of elections is absolutely essential in this respect, as democratic accountability mechanisms are a precondition for human rights protection.[3] As the judgment rightly notes, the scale of election interference phenomena and the speed of the disinformation campaigns that we are dealing with nowadays have "never [been] seen before" (paragraph 134). This means, in my opinion, that the Court's Article 3 Protocol No. 1 standards should also be further adjusted in light of these new developments. Several Contracting Parties have recently been faced with countless incidents of election interference – all trying to weaken, polarise, erode and destabilise their domestic political and constitutional systems. The present case is about the self-defence of domestic democracies and, indirectly, about the self-defence of the Council of Europe itself. By clarifying standards, the Court can help the Contracting Parties to find solutions of how to become more resilient democracies.

4. The standards used by the Court need to be clarified in the following points:

(I) There are three categories of measures of how states can react to foreign electoral interference: (a) measures which are prohibited by the Convention (e.g., foreign agent laws),[4] (b) measures which are acceptable/allowed (but not required), as far as they are proportionate,[5] and (c) measures which are required as positive obligations under Article 3 Protocol No. 1. The standards of these three separate categories need to be clearly defined in order to allow the Contracting Parties to respond appropriately, and the Court needs to give more guidance, especially concerning the last category.

Following the Court's case-law, the judgment rightly emphasises the positive obligations of the Contracting Parties to take measures to ensure the free expression of the opinion of the people in the choice of the legislature. The judgment even lists (as good examples) a number of UK measures that were taken after the elections concerned (paragraphs 169-171). Some of these measures, however, might actually be seen not simply as good practices, but even as positive obligations following from Article 3 Protocol No. 1. As the judgment describes these measures as "address[ing] the points raised by the applicants" (paragraph 172), it should also be clarified how far they may be considered as fulfilling positive obligations under Article 3 Protocol No. 1.

(II) The origin of external influence in electoral processes does matter when assessing the proportionality of defensive measures and the fulfilment of positive obligations. One should differentiate between interferences from non-democratic countries (i.e., states rejecting the founding principles of the Council of Europe, like Russia in the present case) and democratic countries (i.e., states accepting the founding principles of the Council of Europe, potentially also from outside of Europe). The reference to a "democracy capable of defending itself" (paragraphs 114-115) might be a good starting point for this doctrinal differentiation. Membership in the Council of Europe is a helpful (but, unfortunately, nowadays imperfect) indicator in this matter, as some of the Contracting Parties have experienced a substantial erosion of their rule of law and democracy in recent years. The differentiation should therefore also consider the *de facto* quality of liberal democracy in the country from which the external influence originates, for which (besides membership in the Council of Europe) further factors could also be weighed, such as information about the execution of the Court's judgments, systemic deficiencies identified in the Court's judgments, ongoing Article 7 Treaty on European Union procedures (if it is an EU Member State), or widely recognised rule of law and democracy indices (such as the V-DEM Liberal Democracy Index or the World Justice Project Rule of Law Index).[6] The latter could especially be relevant, if a case concerns electoral interference from outside of Europe.

Electoral interference is problematic also if it comes from another democratic country, but it is *especially* problematic if it comes from a non-democratic country (*cf.* above the explanations concerning the original intent of the founding fathers of the Convention). Therefore, the less democratic the origin the interference is, the stronger the defensive measures could and should be. Whether a country is democratic, is not a binary question (yes or no), but a matter of degree: within the framework of a proportionality analysis, this graduality has to be carefully considered.

(III) The judgment rightly points out the close relationship between Article 10 and Article 3 Protocol No. 1 in the context of election interference via digital disinformation (paragraph 161). This relationship is not just a potential conflict, but also complementary and mutually strengthening (i.e., Article 10 and Article 3 Protocol No. 1 need to be interpreted in each other's light, and some positive obligations follow from both).[7] Digital disinformation can reach an extent where the 'noise' level is so high that the right to receive information under Article 10 might be violated. Whereas formerly the Court could consider the internet and social media less impactful than broadcast media,[8] this no longer holds true. While filtering the content of communication before spreading the information is the wrong approach to take, other potential solutions exist.[9] I will only mention a few of them: (a) Article 10 contains, in my opinion, a positive obligation to effectively ensure that social media users know whether information is being spread by real persons using their actual names (regularly

controlled through identity verification, also ensuring a single personal account),[10] real persons using pseudonyms (thereby allowing for anonymity, particularly useful in less democratic environments),[11] groups, fact-checked media companies, other legal persons, or bots. Social media users need to be able to effectively turn down the 'noise' level by *easily* controlling which user category can appear in their news feed, in the comments section and amongst likes.[12] Even if users opt to interact with several account categories at once, they should always be able to easily and immediately see which account belongs to which account category. (b) Moreover, users should by default see in their feeds only those channels which they formerly chose to follow or to which they subscribed to (plus adverts which always explicitly and clearly need to be marked as such); i.e., news feed elements from other channels should only be offered if every time explicitly asked by the users.[13] (c) Slowing down virality by imposing a waiting time (e.g., a few hours) until posts appear. This introduces friction as a counterweight to digital acceleration (except for privileged accounts, such as those of fact-checked media companies).[14] No fact-checking (which is necessarily time-consuming) can resist the overwhelming and saturating flow of disinformation that we are faced nowadays. By the time a piece of disinformation is debunked, it can spread virally through entire social media platforms, and yet a novel piece of disinformation can be launched again. This then repeats itself in an endless loop, wave after wave. (d) Prohibition on micro-targeted political advertisements should also be considered, as such adverts are undermining "free and open democratic debate and equal political participation by all citizens".[15] They are also more susceptible to creating noise levels which strongly interfere with the right of citizens to receive information. (e) The lack of regulations of the influencer marketing space is a gap that malicious non-democratic foreign countries can easily abuse, as we have seen (and are seeing) in various countries both in Europe and outside of it.[16] (f) Requiring the use of blockchain technology for social media news posts could ensure that users can trace the posts back to reliable and fact-checked media sources (if they wish to do so).[17] (g) It is critical that researchers obtain legally guaranteed access to data held by social media platforms in order to reveal social media manipulation practices and techniques. This enables Contracting Parties to strengthen the resilience of their liberal democracies and to effectively protect the Article 3 Protocol No. 1 and Article 10 rights of their citizens.[18] (h) It has been convincingly documented that AI-based chatbots are being purposefully infected by disinformation campaigns.[19] The providers of such services therefore need to be mandated by the Contracting Parties to take special cautionary measures to avoid this.

None of the above specific concrete regulatory solutions follows directly from Article 3 Protocol No. 1 and/or Article 10. There is, however, a positive obligation on Contracting Parties to carefully consider and weigh various regulatory options (such as the above-mentioned ones) in a transparent process in light of these rights, and to update their respective regulations in regular intervals.[20]

One of the strengths of liberal democracies when compared to autocracies is that liberal democracies' political decisions and democratic accountability mechanisms (such as elections) tend to be relatively more strongly influenced by fact-based discourses weighing arguments. If we allow the digital disinformation noise levels to ravage as high as they currently are in our public debates, then we are endangering liberal democracies' structural superiority.

(IV) The question of victim status in many election interference cases is analogous to secret surveillance cases (such as *Szabó and Vissy v. Hungary*, no. 37138/14, § 32–39, 12 January 2016), as one

of the peculiarities is exactly that mostly you cannot be sure how much influence such *covert operations* actually had on the outcome of the elections. Moreover, there is also a trade-off: the stricter we handle the substantive side of the victim status (i.e., actual harm or disadvantage suffered), the stronger the arguments become for a self-standing procedural obligation to investigate. We would otherwise hollow out this right (Article 3 Protocol No. 1) in the present election interference context, as private persons just do not have the IT, logistical and investigative capabilities to acquire and present more evidence on their own.

5. Even though election interference through digital disinformation concerns the heart of the Court's mission of protecting the institutional system of liberal democracy, the respective case-law has so far been much less detailed than in other areas which are less central for this mission. I therefore consider a more developed elaboration of the above questions by the Court urgently necessary.

---

[1]https://commission.europa.eu/topics/strategic-communication-and-tackling-disinformation_en. Last accessed on 13 November 2024.

[2] Angelika Nussberger, *The European Court of Human Rights,* Oxford University Press 2020, p. 189: "The ECtHR had been created to prevent a backlash into dictatorship." The Convention was originally also meant by some of its founding fathers as a collective pact against totalitarianism, see Ed Bates, *The Evolution of the European Convention on Human Rights,* Oxford University Press 2010, p. 75.

[3] On this interconnectedness, see also the Preamble of the Convention: "[…] fundamental freedoms which are the foundation of justice and peace in the world and are best maintained on the one hand by an effective political democracy and on the other by a common understanding and observance of the Human Rights upon which they depend." On the interconnectedness in general, see András Jakab, What Can Constitutional Law Do against the Erosion of Democracy and the Rule of Law? On the Interconnectedness of the Protection of Democracy and the Rule of Law (2020) *Constitutional Studies* vol. 6. pp. 5–34.

[4] *Novaya Gazeta and others v. Russia*, nos. 11884/22 and 161 others, 11 February 2025; *Kobaliya and others v. Russia,* nos. 39446/16 and 106 others, 22 October 2024; *Ecodefence and others v. Russia*, nos. 9988/13 and 60 others, 14 June 2022.

[5] *Parti nationaliste basque – Organisation régionale d'Iparralde v. France*, no. 71251/01, § 43, 7 September 2007.

[6] On rule of law indices and the *de facto* quality of liberal democracy, see András Jakab – Lando Kirchmair, *Saving the European Union from Its Illiberal Member States*, Oxford University Press 2025, pp. 92–123.

[7] On Article 10 positive obligations concerning the right to receive information in the context of personalised news feeds, see Sara Eskens – Natali Helberger – Judith Moeller, Challenged by News Personalisation: Five Perspectives on the Right to Receive Information (2017) *Journal of Media Law* 9(2) pp. 259–284. On Article 3 Protocol 1 positive obligations, see Ethan Shattock, Free and Informed Elections? Disinformation and Democratic Elections Under Article 3 Protocol 1 of the ECHR (2022) *Human Rights Law Review* 22 pp. 1–25, esp. 19.

[8] *Animal Defenders International v. the United Kingdom* [GC], no. 48876/08, § 119, 22 April 2013.

[9] For general overviews with further references, see e.g. Esma Aïmeur – Sabrine Amri – Gilles Brassard, Fake news, disinformation and misinformation in social media: a review (2023) *Social Network Analysis and Mining* 13(30) pp. 1–30; Anastasia Kozyreva et al., Toolbox of individual-level interventions against online misinformation (2024) *Nature Human Behaviour* 8, pp. 1044–1052. For an ongoing UK parliamentary inquiry into the links between algorithms used by social media and search engines to rank content, generative AI, and the spread of harmful or false content online, see https://committees.parliament.uk/work/8641/social-media-misinformation-and-harmful-algorithms/.

[10] William Marcellino et al, *The Rise of Generative AI and the Coming Era of Social Media Manipulation 3.0,* RAND Corporation 2023, p. 26.

[11] Cf. on the necessity of balancing concerning anonymity in order to protect the speaker, see *Delfi AS v. Estonia* [GC], no. 64569/09, § 147–149, 16 June 2015. In the context of the present case, however, we should also consider how to protect the audience from the noise.

[12] On the role of likes for the credibility of news, see Mufan Luo – Jeffrey T Hancock – David M Markowitz, Credibility perceptions and detection accuracy of fake news headlines on social media: effects of truth-bias and endorsement cues (2022) *Communication Research* 49(2) pp. 171–195.

[13] See the proposal by MEPs to the European Commission to apply the Digital Services Act for this purpose, critically analysed by Doris Bujis, The DSA, disinformation and the European elections: solutions through recommender systems?, *DSA Observatory* 17 June 2024: "turning off personalised recommender systems by default for the very large online platforms" and "explicitly stop recommender systems based on interaction".

[14] On friction as a tool to slow virality in general, see Beatriz Botero Arcila – Rachel Griffin, *Social media platforms and challenges for democracy, rule of law and fundamental rights*, Study requested by the LIBE Committee of the European Parliament, 2023, p. 89.

[15] Ibid. p. 126.

[16] R. Gondor Rinderknecht, There's less social media transparency and, likely, more disinformation, *The Hill*, 17 September 2024.

[17] Marcellino *op. cit.* p. 26.

[18] Sinan Aral – Dean Eckles, Protecting Elections from Social Media Manipulation, 365(6456) *Science*, 30 August 2019.

[19] For data and more details, see, e.g., the reports by the Digital Forensic Research Lab (DFRLab) at the Atlantic Council, available at https://dfrlab.org/the-pravda-network/. For reports in daily news, see, e.g., Jacob Judah – Fiona Hamilton, Russia using AI to target Britons with flood of fake news, *The Times* 29 April 2025; Miruna Coca-Cozma, La désinformation russe s'infiltre dans les réponses des assistants virtuels dopés à l'IA, *Radio Télévision Suisse (rts.ch)* 22 June 2024; Joseph Menn, Russia seeds chatbots with lies. Any bad actor could game AI the same way, *Washington Post* 17 April 2025.

[20] Regulation does not necessarily mean direct unilateral state legislation, but also mandated, supervised, obligatory (i.e., without the possibility of opt-out) and sanctioned self-regulation and co-regulation are options (see, e.g., Judit Bayer, *Digital Media Regulation within the European Union: A Framework for a New Media Order*, Nomos 2024, p. 214), if the adoption conforms with the above-mentioned procedural standards.