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

Conference The European Convention of Human Rights at 70: Milestones and Major Achievements

Human Rights and Technological Developments

Speech by Síofra O'Leary

Strasbourg, 18 September 2020

I - Introduction

We gather today to celebrate a Convention adopted in 1950 at a time when it would have been impossible for its authors and signatories to foresee the many different and, in recent years, very rapid technological advances which affect quite profoundly the lives of billions of individuals and society at large.

After all, nineteen years still had to pass before Armstrong's « giant leap for mankind »; a further twenty-six years or more would elapse before an apple came to represent something more than an Autumn fruit, and it was only in the 1980s that telephones became mobile devices available to a small cohort not yet known as the 1 %. Film buffs will remember corporate raider Gordon Gekko on his brick like mobile phone in *Wall Street*.

Fast forward seventy years from the signing of the Convention and my German kitchen robot can now track what I cook, when I cook it but, thankfully, not how well or poorly I do so. The Snapchat app, with 238 million daily active users, allows our teenagers to locate, down to the street name and house number, where their friends are at any given time on a map of the world. By the time the 58th US presidential election takes place in November 2020, the present White House incumbent will have over 80 million followers on Twitter. He will also have demonstrated how a modern social medium which limits users to 280 characters can nevertheless be used not only *by* the press but also to *bypass* the press, and even to develop or communicate government policy.

In a wonderful series of dos and don'ts, written for young scholars, Professor Joseph Weiler highlights the perils of papers presented by members of panels for the conference audience, the moderator and for the speakers themselves.[1] A packed programme, like today, leaves us grappling to try to address complicated questions in 10 to 15 minutes. The result can be an over-ambitious or over-intricate presentation, which overshoots the time slot, stresses the moderator and deprives the audience of their right to exchange and probe. Since the subject matter of my slot — human rights and technological developments – could occupy an entire day or days, I approached the task of preparing this paper with some trepidation. My oral presentation was limited to a *tapas* style menu

[1] See J.H.H. Weiler, "On my way out: Advice to Young Scholars I: Presenting a Paper in an International (and National Conference)" *EJIL:Talk!*, 8 September 2015.

plan — three or four bite size pieces of law and jurisprudence, with a more extensive examination of the subject left to this written paper.

Ever since its landmark ruling in *Tyrer v. the United Kingdom*, the Court has approached the Convention as a living instrument. It must be interpreted evolutively in the light of present-day conditions.[2] As such, the Court has been well-placed to identify and respond over time to change, whether technological or scientific, the latter being the subject of the intervention by my friend and colleague, Judge Pastor Vilanova.

However, when it comes to technological developments and human rights law, it strikes me as too early in relation to *most* Convention articles to speak of "milestones" and "major achievements". Domestic courts, the Court itself and thus the Convention system are, in the main, still feeling their way through the legal, societal and political changes which technological developments necessarily entail. As regards the Court, at least two factors – the rule on exhaustion and the sizeable docket – mean that it takes time for certain legal questions to make their way *to* Strasbourg and, one must be honest, it takes time for the Court to answer many of them. Indeed, we need to be acutely aware that we are insufficiently rapid when providing answers to emerging legal questions themselves the product of rapid technological change, which is not set to cease.

So what aspects of the Convention will I address on this 70th anniversary?

It's commonplace that the digital era in which we now live has had significant legal effects primarily in two areas of Convention law: freedom of expression, protected by Article 10, which also covers the right to receive and impart information, and the right to respect for private life guaranteed by Article 8. Think of the endorsement of the internet as one of the principal means of expression in *Ahmet Yildirim v. Turkey*, or recognition of the risks it entails in *Editorial Board of Pravoye Delo and Shtekel v Ukraine*. Think of the establishment of safeguards and protection regarding the use of geolocation devices by State actors in *Uzun* or *Ben Faiza*, the liability of internet news portals for customer comments in *Delfi v. Estonia*, or even the all essential balancing of expression and privacy rights when it comes to the right to be forgotten the subject of *M.L. and W.W. v. Germany*, to name but a few.

However, today I prefer to concentrate on Convention articles which have been treated as more peripheral in discussions relating to the consequences for human rights of technology and digitalisation:

- jurisdiction within the meaning of Article 1 of the Convention (II);

- challenges posed by technological advances for the judicial process itself, given the standards in Article 6 (III);

- legal questions which may arise in relation to the right to free elections, guaranteed by Article 3 of Protocol n° 1 (VI), and

- the consequences, if any, in a digitally dependent world, for the right not to be deprived of an education in Article 2 of Protocol n° 1 (VII).

[2] *Tyrer v. the United Kingdom*, no. 5856/72, 25 April 1978.

II - The challenges posed by technological developments to the notion of jurisdiction within the meaning of Article 1 ECHR[3]

Article 1 of the Convention provides that:

> "The High Contracting Parties shall secure to everyone within their jurisdiction the rights and freedoms defined in Section I of the Convention".

The exercise of jurisdiction – a threshold criterion – is a necessary condition for a Contracting Party to be held responsible for acts or omissions imputable to it which give rise to an alleged violation of the Convention.[4] This Article 1 notion of jurisdiction has been pivotal in determining who ECHR right-holders and duty-bearers are.[5]

The basic principle established by Article 1 is that a State's jurisdictional competence is *primarily* territorial. Furthermore jurisdiction is presumed to be exercised normally throughout a State's territory.[6] Over time the Court has recognized that acts performed or producing effects outside the Contracting States' territories can constitute an exercise of Article 1 jurisdiction. However, this is said to occur only in exceptional cases.[7] Situations in which extraterritorial jurisdiction has been established have to date been arranged roughly into two baskets – the exercise of State control and authority over an individual[8] and the exercise of effective control over an area outside territorial boundaries as a consequence of lawful or unlawful military action or through a subordinate local administration.[9]

The internet and online information, without which, as we discovered during this year's global pandemic, our society no longer functions effectively are:

> "geographically independent: they avoid physical borders and, by their nature, operate on a cross-border basis. This characteristic can clearly be perceived from two aspects: cross-border flow of information and worldwide accessibility".[10]

How, therefore, can and should a Court which has determined State responsibility with reference to a primarily territorial concept of jurisdiction accommodate the transnational, borderless reality of the digital sphere?

Although the ECtHR is only beginning to feel its way regarding the question of jurisdiction and the digital sphere, it would be a mistake to consider that the topic is entirely new to the case-

[3] For a more detailed analysis of questions relating to jurisdiction in a digital age variously S. O'Leary, "Data protection and privacy questions in the digital age: whither jurisdiction and the ECHR?" in *Human Rights Challenges in the Digital Age: Judicial Perspectives* (Council of Europe, 2019) 93-122 and the material cited therein.

[4] *Al-Skeini and others v. the United Kingdom* [GC], no. 55721/07, 7 July 2011 § 130; *Ilaşcu and Others v. Moldova and Russia* [GC], no. 48787/99, 8 July 2004, § 311, and *Catan and Others v. Moldova and Russia* [GC], nos. 43370/04 18454/06 8252/05, 19 October 2012, § 103.

[5] See S. Besson, "The extraterritoriality of the ECHR: why human rights depend on jurisdiction and what jurisdiction amounts to" (2012) 25 *Leiden Journal of International Law* 857, 860.

[6] *Banković and Others v. Belgium and Others* (dec.) [GC], no. 52207/99, 12 December 2001, §§ 61 and 67, and *Assanidze v. Georgia* [GC], no. 71503/01, 8 April 2004, § 139.

[7] See, for a short and topical overview of the relevant principles, *Chagos Islanders v. the United Kingdom*, no. 35622/04, 11 December 2012.

[8] See *Jaloud v. the Netherlands* [GC], no. 47708/08, 20 November 2014.

[9] *Assanidze v. Georgia* [GC], cited above, § 139.

[10] See E. Márton, *Violations of Personality Rights through the Internet: Jurisdictional Issues under European Law* (Nomos 2015) 56.

law. In some earlier data protection and surveillance cases, the Court examined alleged interferences with Article 8 rights located within the territory of the respondent State, albeit the person or persons whose rights were affected were located elsewhere. In *Weber and Saravia v. Germany*, for example, a case decided in 2006, the applicants resided in Uruguay while the interception of communication – the subject of the application – occurred in Germany.[11] The Court dismissed the complaint under Article 8 as manifestly ill-founded, rendering it unnecessary to examine the respondent Government's objection that the case was outside its jurisdiction pursuant to Article 1 as defined in *Banković*. The German government had argued that the monitoring of telecommunications made from abroad had to be qualified as an extraterritorial act. One of the applicants had countered that she came within German jurisdiction as she was a German national and both applicants had argued that it could not be decisive that the impugned acts had taken effect abroad.[12] In *Liberty and Others v. the United Kingdom*[13], decided two years later, the communications which were intercepted in the United Kingdom were between two organisations located in Ireland and a third one located in the United Kingdom. In this case no question relating to Article 1 jurisdiction was raised either by the respondent States or by the Court.[14]

Questions relating to jurisdiction are now centre stage. The applicants in *Big Brother Watch*, which is pending before the Grand Chamber following referral of the case pursuant to Article 43 of the Convention, complain about the scope and scale of electronic surveillance programmes operated by the authorities of the respondent State.[15] They argue that previously applicable domestic law was incompatible with the Convention since it authorised interferences with their Article 8 privacy rights by making possible, in the absence of appropriate procedures and safeguards, *inter alia*, the bulk interception of communications and intelligence sharing with foreign governments.

As regards the bulk interception regime, the Chamber noted that while the respondent government contested the alleged interference, they did not raise any objection under Article 1 of the Convention; nor did they suggest that the impugned interception of communications was taking place outside the United Kingdom's territorial jurisdiction. As a consequence, the Chamber proceeded on the assumption that the matters complained of in relation to bulk interception fell within the jurisdictional competence of the United Kingdom.[16] As I'm not a member of the Grand Chamber formation I can perhaps ask whether it is not worth reflecting on whether the Court can or should proceed on the basis of such an assumption; the question of its jurisdiction *ratione personae* being one which it can and does raise of its own motion.[17]

---

[11] *Weber and Saravia v. Germany* (dec.), no. 54934/00, 29 June 2006.
[12] Ibid, §§ 66 et seq.
[13] *Liberty and others v. the United Kingdom*, no. 58243/00, 1 July 2008.
[14] See the discussion in M. Milanović, "Human Rights Treaties and Foreign Surveillance: Privacy in the Digital Age" (2015) *Harvard International Law Journal* 82, 127.
[15] *Big Brother Watch and Others v. the United Kingdom*, nos. 58170/13, 62322/14 and 274960/15, 13 September 2018. See also, for a related case referred at the same time and also pending, *Centrum för Rattvisa v. Sweden*, no. 35252/08, 19 July 2018.
[16] *Big Brother Watch and Others v. the United Kingdom*, cited above, § 271.
[17] The IPT, (2016) UKIPTrib 15, judgment of 16 May 2016, had ruled (§ 58), that as regards persons located outside the UK but who claimed to have been surveilled by the UK, none of them had alleged that they had a private life in the UK. Accordingly, the IPT held, "under Article 1 the UK was under no obligation to respect it". According to Milanović, the UK's failure to raise a jurisdiction objection is to be welcomed as it allowed the competent ECtHR Chamber to avoid the whole issue and proceed on the basis of the assumption described above (M. Milanovic, "ECHR Judgment in Big Brother Watch v. UK", *EJIL:Talk!,*17 September 2018, <https://www.ejiltalk.org/ecthr-judgment-in-big-brother-watch-v-uk/> accessed 2 October 2019).

The 2018 Chamber judgment in *Big Brother Watch* also marked the first occasion on which the Court addressed the issue of the compliance of an intelligence sharing regime with Article 8 ECHR. The applicants claimed that the authorities of the respondent State requested and received intelligence from US intelligence services operating within the framework of the surveillance programmes managed by the latter country. One of the third party interveners, the International Commission of Jurists (ICJ), submitted before the Chamber that the fact that, in a mass surveillance operation, elements of the interference with rights might take place outside a State's territorial jurisdiction didn't preclude that State's responsibility, since its control over the information was sufficient to establish jurisdiction.[18] The Chamber held that the interference under consideration did not lie in the interception itself, given that it did not occur within the UK's jurisdiction but was carried out under the full control of the US' authorities. Rather, the interference lay in the receipt of the intercepted material and its subsequent storage, examination and use by the intelligence services of the UK:

> "[I]t is important to clarify at the outset the nature of the interference under consideration [occasioned by the existence of an intelligence sharing regime in which the respondent State participated].
>
> Although the impugned regime concerns intercepted communications, the interference under consideration in this case does not lie in the interception itself, which did not, in any event, occur within the United Kingdom's jurisdiction, and was not attributable to that State under international law. As the communications are being intercepted by foreign intelligence agencies, their interception could only engage the responsibility of the respondent State if it was exercising authority or control over those agencies (see, for example, *Jaloud v. the Netherlands* [GC], no. 47708/08, §§ 139 and 151 ECHR 2014 and *Al-Skeini and Others v. the United Kingdom* [GC], no. 55721/07, §§ 130-139, ECHR 2011). Even when the United Kingdom authorities request the interception of communications (rather than simply the conveyance of the product of intercept), *the interception would appear to take place under the full control of the foreign intelligence agencies*. […].
>
> Consequently, *the interference lies in the receipt of the intercepted material and its subsequent storage, examination and use by the intelligence services of the respondent State*."[19]

The Chamber went on to assess the quality of the legal basis in the respondent State for intelligence sharing having regard to the requirements established in the Court's existing case-law and found that the domestic law was compliant with Article 8 requirements.[20]

One will have to wait and see if and how the Grand Chamber tackles questions in relation to jurisdiction in its forthcoming judgment. In this ever-changing and increasingly crowded legal and judicial space, the Grand Chamber will be deliberating against the background of several European and domestic court decisions of relevance handed down over the last year. In 2019, in *Google LLC (successor to Google Inc.) v. CNIL*, the CJEU clarified further the territorial scope of the Data Protection Directive.[21] The key question in the case was whether the "right to be forgotten", namely

[18] *Big Brother Watch and Others v. the United Kingdom*, cited above, § 299.
[19] Ibid, §§ 419-421 (emphasis added).
[20] Ibid, §§ 425-444.
[21] Case C-507/17, *Google LLC (successor to Google Inc.) v. CNIL*, EU:C:2019:772.

the right of a person to have internet links dereferenced by the operator of a search engine, operates on a national, European or worldwide level?[22] The CJEU opted for an intermediate EU wide solution. It held that, the internet being a global network without borders, the referencing of a link referring to information regarding a person whose centre of interests is in the EU is likely to have immediate and substantial effects on that person.[23] According to the CJEU, considerations of this nature are such as to justify the existence of a "competence" on the part of the EU to lay down a dereferencing obligation on all versions of its search engine.[24] However, numerous third States do not recognize the right to be forgotten/the right to dereferencing or have a different approach to it. Moreover, the balance between privacy and data protection rights and the freedom of information of internet users is likely to vary significantly around the world. The CJEU held that the EU legislature had not (yet) struck a balance between the aforementioned rights and freedom as regards the scope of dereferencing outside the Union, something which it has done so far as the Union itself is concerned. As a result, a search engine cannot, according to the CJEU, be required under EU law to carry out dereferencing on all versions of its search engine, although EU law does not currently prohibit such a practice.[25] As EU law stands, therefore, the 1995 Directive and the GDPR require a search engine operator, when granting a dereferencing request, to carry this out:

> "on the versions of the search engine corresponding to all the Member States [of the EU], using, where necessary, measures which, while meeting the legal requirements, effectively prevent or, at the very least, seriously discourage an internet user conducting a search from one of the Member States on the basis of a data subject's name from gaining access, via the list of results displayed following that search, to the links which are the subject of that request".[26]

Glawischnig-Piesczek v. Facebook Ireland Limited, another CJEU judgment, concerned the territorial scope of an injunction issued by an Austrian court to an Austrian politician ordering Facebook to remove defamatory posts.[27] The question before the referring Austrian Supreme Court was whether the injunction against a host provider which operates a social network with a large number of users may also be extended worldwide to statements with identical and/or having equivalent content of which Facebook is not aware. Since the e-commerce Directive does not regulate the territorial scope of an obligation to remove information disseminated via a social

[22] In *Google LLC* the President of the French Data Protection Authority, the CNIL, served formal notice on Google LLC that, when it granted the request of a natural person seeking the removal of links to web pages from the list of results displayed following a search carried out on the basis of his name, it must apply that removal to *all* the domain name extensions of its search engine. Google refused to comply with that notice, merely removinge the links in question from the results displayed in response to searches carried out on versions of its search engine whose domain name corresponds to an EU Member State. The parties before the CJEU were divided on the subject of a worldwide dereferencing requirement: §§ 34-35 of the Opinion of Advocate General Spuznar, C-507/17, *Google LLC v. CNIL*, EU:C:2019:15. The CNIL, the French Défenseur des droits, France, Italy and Austria all argued for a requirement of worldwide dereferencing in order to ensure the effectiveness of the rights conferred by the Directive; a position shared by the Article 29 Working Party on Data Protection. In contrast, the European Commission, Ireland, Greece, Poland, Google and a series of freedom of expression NGOs argued against a worldwide right to dereferencing on the basis of EU law as, in their view: "it would not be compatible with either EU law or public international law and would amount to a dangerous precedent that would invite authoritarian regimes also to require the implementation of a worldwide scale of their censorship decisions."

[23] § 57 of the judgment in *Google LLC*, cited above.

[24] Ibid, § 58.

[25] Ibid, §§ 59-72.

[26] Ibid, § 73.

[27] Case C-18/18, *Glawischnig-Piesczek v. Facebook Ireland Limited*, EU:C:2019:458 (Opinion) and EU:C:2019:821 (judgment), commented in a blogpost on

<http://eulawanalysis.blogspot.com/2019/05/facebook-defamation-and-free-speech.html> accessed 11 September 2020. See § 12 of the Opinion for details of the publication on the user's personal page of an article from a news magazine, the generation on Facebook of a thumbnail of the original site and the user's accompanying disparaging comments.

network platform,[28] the CJEU held that it did not preclude a host provider from being subject to an injunction with worldwide effects. According to the CJEU, it was up to Member States to ensure that measures, such as injunctions, which they adopt and which produce worldwide effects take due account of "the rules applicable at international law". Also touching on questions of extra-territorial effects, in *Schrems II*, handed down in July 2020, the CJEU invalidated the Commission's Privacy Shield Decision because of its failure to ensure transfers of data to the U.S. were guaranteed an adequate level of protection.[29]

Meanwhile, in May 2020, the German Federal Constitutional Court handed down a landmark ruling on questions of jurisdiction and fundamental rights protection in the field of data protection. It held that the Federal Intelligence Service is bound by the fundamental rights of the Basic Law when conducting telecommunications surveillance of foreigners in other countries. The constitutional protection applies irrespective of whether surveillance is conducted from within Germany or from abroad. According to the German court:

> "No restrictive requirements that make the applicability of fundamental rights dependent on a territorial connection with Germany or on the exercise of certain sovereign powers can be inferred either from the provision itself or its legislative history or position in the systematic framework of the Basic Law. Rather, the Basic Law's aim to provide comprehensive fundamental rights protection and to place the individual at its centre entails that fundamental rights as rights of the individual ought to provide protection whenever the German state acts and thus potentially creates a need for protection – irrespective of where, towards whom and in what manner it does so. In any event, this holds true for fundamental rights affording protection against surveillance measures as rights against state interference, which are at issue in the present case."[30]

As indicated previously, the Grand Chamber will address Article 1 jurisdiction questions in the *Big Brother* case against the background of this ever richer judicial tapestry.[31]

Most legal commentators seem to agree on one thing when it comes to questions relating to jurisdiction - the effective control test developed to date by international human rights courts, including the ECtHR, to determine jurisdiction is unsuitable in the context of the digital sphere and, in particular, in relation to state-sponsored cyber surveillance. In the words of one commentator, it does not cover all the odd ways and forms that state power now travels and effects rights of

[28] See Directive 2000/31 of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the internal market (OJ L 178/1).

[29] Case C-311/18, *Data Protection Commissioner v. Facebook Ireland Limited and Maximillian Schrems*, EU:C:2020:559.

[30] Taken from Press Release no. 37/2020 of 19 May 2020 in relation to the judgment of 19 May 2020, 1 BvR 2835/17.

[31] Other Article 8 surveillance cases raising jurisdictional issues are also in the pipeline. The applicants in *Privacy International and Others v. the United Kingdom* are a UK NGO, internet service providers registered in the UK, US and South Korea and an association of "hacktivists" registered in Germany. They claim that their equipment has been subject to interference known as "Computer Network Exploitation or Equipment Interference" – colloquially known as "hacking" – over an undefined period by the UK Government Communications Headquarters (GCHQ) and/or the Secret Intelligence Service (SIS). The alleged interference is alleged to have been based on section 7 of the 1994 Intelligence Services Act which allows the Secretary of State to authorize a person to undertake (exempt from liability) an act outside "the British Islands" to which they would be held liable if it were done in the UK. During the domestic proceedings before the Investigatory Powers Tribunal (IPT) the respondent government accepted or avowed the use of equipment interference. However, does the UK's jurisdiction extend to authorisations of equipment interference undertaken outside the United Kingdom? Noting that jurisdiction under the Convention is territorial except in exceptional cases, the IPT reserved its position on the question of jurisdiction and the applicability of the Convention. In the pending Convention proceedings one of the questions communicated asks whether the facts of which the applicants complain occur within the jurisdiction of the United Kingdom (See *Privacy International and Others v. the United Kingdom*, no. 46259/16, communicated on 19 November 2018).

individuals extraterritorially.[32] Various alternative models to effective control, some more and some less concrete in terms of their content and effects have been advanced. One is a virtual control test, understood as remote control over the individual's right to the privacy of his or her communications. Establishing virtual control would depend not on where the interference takes place but rather on whether or not the State can assert such control (the ability to intercept, store, analyse and use communications) even when it lacks authority or control over the territory or the physical person.[33] A second proposal concerns interface-based jurisdiction, which would occur where data or communications are intercepted within a State's territory, with the result that the latter owes obligations to the individuals whose data has been intercepted, regardless of the location of those individuals. The State obligation in such cases would be one not to interfere with individuals' data and communications.[34] Some would argue that this is not a million miles away from the approach chosen by the Chamber in *Big Brother Watch*, albeit the applicant organisations in that case were themselves established in the UK. A not dissimilar proposal by Milanovic is based on the distinction between a State's positive obligation to secure human rights and its negative obligation to respect them. Writing in the context of foreign surveillance, he argues that the existence of positive obligations must be predicated on a State having effective overall control over an area. In contrast, a negative duty to refrain from interference would apply to all potential victims of foreign surveillance activities. Such an obligation would be "territorially unlimited and not subject to any jurisdictional threshold, because any such threshold that was non-arbitrary would collapse anyway".[35] Other commentators argue that the distinction between territorial and extraterritorial jurisdiction in the field of data protection should make way for other criteria such as a substantial connection between the subject matter of the litigation or damages suffered and the jurisdiction issuing a judgment or order. They point to the 1935 Harvard Draft Principle, which was designed for law enforcement matters, which is posited on such a substantial connection combined with the State seeking to exercise jurisdiction having a legitimate interest in the matter.[36]

As I indicated in the introduction, it is impossible in the digital field and in relation to jurisdictional questions of this nature to speak in terms of milestones and achievements by the ECtHR. With several cases pending where jurisdictional questions arise, we see in fact that there are far more questions than judicial answers presently available. The living instrument doctrine is not simply inspired by present-day conditions, which change over time, but also by developments in international law and by what could be regarded as a principle of ECHR effectiveness, namely the need to reflect an increasingly high standard in the area of protection of human rights, necessitating greater firmness in assessing breaches of the fundamental values of democratic societies.[37] As such,

---

[32] See B. Çali, "Has 'Control over rights doctrine' for extra-territorial jurisdiction come of age? Karlsruhe too, has spoken, now it's Strasbourg's turn" *EJIL:Talk!,* 21 July 2020, <https://www.ejiltalk.org/has-control-over-rights-doctrine-for-extra-territorial-jurisdiction-come-of-age-karlsruhe-too-has-spoken-now-its-strasbourgs-turn/> accessed 11 September 2020.

[33] See, *inter alia*, E. Watt, "The Role of International Human Rights Law in the Protection of Online Privacy in the Age of Surveillance" in H. Röigas et al (eds) *Defending the Core* (9th International Conference on Cyber Conflict 2017 Tallinn, Estonia) 1-14 and P. Margulies, "The NSA in the Global Perspective: Surveillance, Human Rights and International Counterterrorism" (2014) 82 *Fordham Law Review* 2137.

[34] C. Nyst, "Interface Based Jurisdiction Over Violations of the Right to Privacy", 21 November 2013, *EJIL:Talk!*, <https://www.ejiltalk.org/interference-based-jurisdiction-over-violations-of-the-right-to-privacy> accessed 2 October 2019.

[35] M. Milanovic, cited above, 119.

[36] See M. Catanzariti, "Off-line Digital Jurisdiction" EUI WP RSCAS 2019/03, 11 and D.J.B. Svantesson, "A new jurisprudential framework for jurisdiction: beyond the Harvard Draft" (2015) 109 *American Journal of International Law* 69 – 74. Kuner posits a similar "effects" doctrine in the context of EU law (C. Kuner, "The Internet and the Global Reach of EU Law", LSE Law Society and Economy Working Papers 4/2017, 33), citing *Air Transport Association of America* (C-366/10, EU:C:2011:864, §§ 122-127).

[37] See, for example, for this facet of the living instrument doctrine, *Demir and Baykara v. Turkey* [GC], no. 34503/97, 12 November 2008, § 146 or *Selmouni v. France* [GC], no. 25803/94, 28 July 1999, § 101. On reliance on the principle of « effectiveness » as a tool or requirement when interpreting the ECHR see *Selmouni v. France*, cited above, § 101; *Siliadin v. France*, no. 73316/01, 26 July 2005, §§ 121-129; *Rantsev v. Cyprus and Russia*, no. 25965/04, 7 January 2010, §§ 272-282.

one could argue that growing pressure to adapt is building as a result both of the nature and extent of the technological developments at issue and the recent decisions at European and national level seeking to respond to those changes in cases relating to Article 8, privacy and data protection. The development of the Court's case-law on Article 1 to date suggests, in the words of one author, that thus far it has been "well aware of the risks inherent in asserting a global approach to jurisdiction".[38] At the same time, the challenge ahead will be to avoid Convention overreach while preventing the development of black holes in human rights protection which develop precisely because of the transnational nature of the digital sphere or because States and indeed private companies seek to exploit the absence of regulatory reach in order to circumvent human rights protection.[39] The judgment of the German Federal Constitutional Court was posited on recognition of the expanding sphere of action of the German State and the need to avoid just such an accountability gap in relation to the exercise of public power which produces extraterritorial effects. It has been read by some commentators as possibly "nudging" Strasbourg towards a revision, in a digital context at least, of its two effective control exceptions.[40]

III - Technological developments and the judicial process

Article 6 ECHR enshrines the right to a fair trial and through its case-law thereunder the Court has, over decades, established common standards for the functioning of the judicial systems of 47 Member States.

As discussed at a conference of Ministers of Justice of the Council of Europe, held in October 2019, the constant innovation of technologies has led domestic and European judicial systems and legal professions to confront and manage new challenges and opportunities. Access to justice, for example, can be greatly facilitated by online services which facilitate registration and inform individuals economically and efficiently of their rights and of the relevant procedures to be followed. Automated case management, advanced search engines and electronic case analysis are digital tools without which we might no longer know how to perform our jobs properly or at speed. A global pandemic both confirmed this and provided the incentive for further change, as deliberations and hearings went online; albeit accompanied by glitches which remind us that regardless of technological advances, we remain very human.[41] The aforementioned Council of Europe conference sought to reflect on how the fundamental principles which must guide judicial systems and fair trial guarantees can be safeguarded while accommodating digital advances.

That is not, however, the issue which interests me for the purpose of the present discussion of Convention milestones and major achievements. I would like to reflect instead on how new technology is affecting judicial life in the courtroom, whether from the perspective of the accused, victims of crime, the judge or trials by jury; referred to by the Court as "persons involved in the

[38] See M. O'Boyle, "The ECHR and Extraterritorial Jurisdiction: A Comment on 'Life after Banković'" in F. Coomans and M.T. Kamminga (eds.), *Extraterritorial Application of Human Rights Treaties* (Intersentia 2004) 128.

[39] A. Nussberger, "The Concept of 'Jurisdiction' in the Jurisprudence of the European Court of Human Rights" (2012) 65 *Current Legal Problems* 241, 267, argues that in all cases where the extraterritorial application has been discussed, the Strasbourg Court was the only available international institution to analyse alleged human rights violations with binding effects for the Parties concerned: "All the applicants – *Hirsi, Al-Skeini, Loizidou* – would have been left without any alternative effective international judicial remedy, if the Court had not decided their cases".

[40] See Çali, cited above.

[41] See, for example, the report in the Irish Legal News, « English child care judge found to have potential bias after leaving remote link open », 31 July 2020, <https://www.irishlegal.com/article/english-child-care-judge-found-to-have-potential-bias-after-leaving-remote-link-open> accessed 11 September 2020, or the interruption of oral arguments by the sound of a flushing toilet in the first US Supreme Court hearing to be streamed online, reported by the BBC on 7 May 2020.

machinery of justice".[42] The digital challenge for the trial process was summarised in the following terms in a UK case involving reporting restrictions:

> "It is beyond argument that members of the public have long held and expressed views about all aspects of the criminal trial process, including the guilt of those facing trial, the gravity of the offending and the appropriate sentence. In the privacy of their homes, or in social gatherings, expressions of such views are part of the discourse of life. What passes in such discussions does not in any way affect the trials about which comment is made and those who might be affected (such as jurors) are unlikely to be involved. … The world has now changed and observations which were previously communicated orally or had the most limited publication now appear on social media sites and are readily accessible by a potentially vast audience."[43]

To my great surprise, I found very few cases before the Strasbourg court reflecting what we know may be increasingly problematic at national level. One of the few exceptions is a case called *Dallas v. the United Kingdom*. The applicant before the Strasbourg court claimed a violation of Article 7 ECHR on account of having been found guilty of a criminal offence (contempt of court for consulting the internet when serving as a juror on a criminal trial) which she claimed had not constituted an offence when it was committed. Contrary to the judge's direction to the jury at the time of its empanelment, the applicant had researched via Internet the previous convictions of the defendant in the pending criminal trial and had informed the other jurors of her findings. The trial judge discharged the jury, the trial was aborted and the applicant was convicted of contempt of court. She claimed that the essential aspects of the defence of contempt under domestic law had not been made out. In finding no violation of Article 7 ECHR, the Court held that the domestic court had not introduced a new test for contempt but rather had clarified as a matter of judicial interpretation the relevant domestic law on the manner in which intent could be proved, albeit in new circumstances. The consequences of contempt of court on account of Internet research had been made clear in notices in the jury room and it had in any event been open to the applicant to clarify the matter of possible sanctions with the trial judge.

The case is an illustration, on the one hand, of the fact that Article 7 of the Convention will not be breached where judicial development of the law in a particular case is consistent with the essence of the offence and could be reasonably foreseen.[44] On the other hand, it illustrates the challenge posed by the Internet when it comes to the protection of Convention rights, in the instant case the need to secure the Article 6 guarantee to a fair trial before an impartial tribunal against the risks which the Internet creates for the introduction of extraneous material into the jury room. The importance of the latter was explained in the following terms a decade ago by the then Lord Chief Justice of England and Wales:

> "If material is obtained or used by the jury privately, whether before or after retirement, two linked principles, bedrocks of the administration of criminal justice, and indeed the rule of law, are contravened. The first is open justice, that the defendant in particular, but the public too, is entitled to know of the evidential material considered by the decision making body; so indeed should everyone with a responsibility for the outcome of the trial, including

[42] *Sunday Times v. the United Kingdom,* no. 6538/74, 26 April 1979, § 56.
[43] See Sir. Brian Leveson P. in *Ex parte British Broadcasting Corporation and others* [2016] EWCA Crim 12, §§ 1-2.
[44] See *Del Rio Prada v. Spain* [GC], no. 42750/09, 21 October 2013, §§ 92-93.

counsel and the judge, (…). This leads to the second principle, the entitlement of both the prosecution and the defence to a fair opportunity to address all the material considered by the jury when reaching its verdict. Such an opportunity is essential to our concept of a fair trial".[45]

Domestic criminal proceedings, in particular in high profile sexual assault and murder cases further demonstrate the risks which the Internet and social media are posing for the accused (particularly if they are minors) and their families, victims and their own families and more broadly the judicial process. I provide one example from my own jurisdiction. In 2019, two Irish teenagers were convicted of the murder of a classmate, and one of the two additionally of aggravated sexual assault.[46] My comments relate in no way to their trial or pending appeal. Both boys were aged 13 when the offence of which they were convicted occurred. Given the nature of the crime and the age of those charged with it, trial was one of the most intensely followed in the history of the State. We saw that in *Dallas v. the United Kingdom* contempt of court proceedings were brought in relation to an identifiable and identified juror. In this case the origin of the alleged contempt occurred in anonymous bedrooms and chatrooms, via keyboards, sends, likes and forwards, executed throughout the land. As the two convicted minors awaited sentencing, contempt and interim injunction proceedings were brought by the Director of Public Prosecutions against Facebook and Twitter. Publication of the identities of child offenders is a criminal offence under domestic law punishable on conviction with up to three years in prison and a €10,000 fine. Interim injunctions were granted compelling the social media companies to remove any posts that identified the two boys that the companies became aware of or were brought to their attention. Granting the injunctions the competent judge sought to explain the unique and sensitive nature of a trial involving children charged with the most serious criminal offence in law and the reason why the relevant domestic legislation provided for the need for a child accused to be treated differently to adults in court in accordance with international treaties on the rights of children:

"This is about the rule of law and the integrity of the trial process. Th(ose who post on social media) must know the seriousness of the activity that they are about."

This is not, unfortunately, an isolated case. In 2016 the Court of Appeal in England heard an appeal in the case referred to above relating to reporting restrictions and a case concerning two teenage girls aged 13 and 14 charged with a murder that provoked public outrage. As a result of a torrent of comments and abuse posted on Facebook and social media, the trial judge felt constrained to discharge the jury and order a retrial at a different venue several months later, creating considerable stress for the family of the victim, the witnesses, the defendants and their families and all those involved in the trial.[47] A reporting restriction originally imposed was lifted and replaced with an order directing media organisations not to place any report on the proceedings on their Facebook profiles and to disable the ability for users to post comments on online articles. In Northern Ireland, in a high-profile rape trial, *R. v Jackson and Others*, involving several international sports stars, interference with the trial by social media posts was manifest, albeit considered insufficiently prejudicial to lead to a discharge of the jury. Not only was the complainant the subject of unlawful identification, but online abusive comments about both her and the accused proliferated

[45] See Lord Judge speaking at the Judicial Studies Board lecture, Belfast, November 2010, reported in the Gillen Review, *Report into the law and procedures in serious sexual offences in Northern Ireland*, April 2019, 221.
[46] Judgment of the Irish High Court, IEHC reference not yet found.
[47] See the trial of *R. v F. and D.* in Leeds Crown Court, 7 April 2016 and the appeal in relation to reporting restrictions in *Ex parte British Broadcasting Corporation and others*, cited above.

throughout the trial. At several points during the hearing, lawyers had drawn to the trial judge's attention online comments, the resolution of which was time-consuming and costly. A defence solicitor was quoted after the trial as saying that several days of the trial had been lost due to issues thrown up by online material and pointed to the distraction of having to monitor online content.[48]

A call for evidence by the then UK Attorney General suggests that trial judges have the tools necessary to manage posts on social media which relate to fair and accurate newspaper reports about ongoing trials. However, while these existing tools, mainly proceedings for contempt, mitigated the risk of serious prejudice, where prejudicial comments appeared on social media separate from newspaper stories, they could not remove it entirely or prevent considerable delay in the trial process. All those interviewed spoke of the need for consolidated guidance for the judiciary and other practitioners regarding the use of contempt of court in such cases.[49]

Pursuant to Articles 6 and 10 of the Convention the Court has of course developed abundant case-law over the decades on the requirements of a fair trial, management of juries by trial judges and the justifiable limits to court room publicity.[50] It has held that a virulent press campaign can adversely affect the fairness of a trial by influencing public opinion and, consequently, the jurors called upon to decide the guilt of an accused.[51] At the same time, press coverage of current events is an exercise of freedom of expression, guaranteed by Article 10 of the Convention.[52] If there is a virulent press campaign surrounding a trial, what is decisive is not the subjective apprehensions of the suspect concerning the absence of prejudice required of the trial courts, however understandable, but whether, in the particular circumstances of the case, his or her fears can be held to be objectively justified.[53] In the context of a trial by jury, the content of any directions given to the jury has been regarded as a relevant consideration and safeguard. However, two things are noticeable about this well-established case-law. Firstly, this case-law on the principle of open justice developed in relation to a concept of a trial, the taking of evidence etc, as something which occurred in a physical place, accessible to the public. It also developed in the knowledge that only a minute section of the public could and would attend the public hearing and that court reporting would be done by professional journalists, in accordance with established rules, and thus by persons themselves subject to professional duties and responsibilities (to which the case-law on Article 10 of the Convention itself refers).[54] In 2020, the sanitary crisis has forced courts across the

[48] See futher details in the Gillen Report, cited above, 252.

[49] See *Response to Call for Evidence on the Impact of Social Media on the Administration of Justice*, March 2019, Attorney General's Office, United Kingdom.

[50] See, as regards publicity and fair trial requirements, *Riepan v. Austria*, no. 35115/97, 14 November 2000, § 27; *Krestovskiy v. Russia*, no. 14040/03, 28 October 2010, § 24 or *Sutter v. Switzerland*, no. 8209/78, 22 February 1984, § 26, according to which the public character of proceedings protects litigants against the administration of justice in secret with no public scrutiny and is one of the means whereby confidence in the courts can be maintained. By rendering the administration of justice visible, publicity contributes to the achievement of the aim of Article 6 § 1, namely a fair trial, the guarantee of which is one of the fundamental principles of any democratic society.

[51] See, for example, *Akay v. Turkey* (dec.), no. 58539/00, 24 October 2006 and *Craxi v. Italy*, no. 34896/97, 5 December 2002, § 98.

[52] *Bédat v. Switzerland* [GC], no. 56925/08, 29 March 2016, § 51.

[53] *Włoch v. Poland* (dec.), no. 27785/95, 19 October 2000; *Daktaras v. Lithuania* (dec.), no. 36662/04, 31 July 2012; *Priebke v. Italy* (dec.), no. 48799/99, 7 March 2002; *Butkevičius v. Lithuania* (dec.), no. 48297/99, 26 March 2002; *G.C.P. v. Romania*, no. 20899/03, 20 December 2011, § 46; *Mustafa (Abu Hamza) v. the United Kingdom* (dec.), no. 31411/07, 18 January 2011, §§ 37-40. Some of the factors identified in the case-law as relevant to the Court's assessment of the impact of such a campaign on the fairness of the trial include: the time elapsed between the press campaign and the commencement of the trial, and in particular the determination of the trial court's composition; whether the impugned publications were attributable to, or informed by the authorities; and whether the publications influenced the judges or the jury and thus prejudiced the outcome of the proceedings (*Abdulla Ali v. the United Kingdom*, no. 30971/12, 30 June 2015, §§ 87-91; *Paulikas v. Lithuania*, no. 57435/09, 24 January 2017, § 59).

[54] In *Riepan v. Austria*, for example, the Court held that a trial complies with the requirement of publicity if the public is able to obtain information about its date and place, and if this place is easily accessible to the public (*Riepan v. Austria*, cited above, § 29).

globe, including the Strasbourg court, to move hearings online, such that public access, if it is possible, is digital and not always live.[55] In addition, leaving Covid aside, by 2020, the imparting of information on criminal trials is no longer the remit of accredited court reporters but has moved online to be performed in a variety of ways by a variety of actors on social media platforms. This leads to the second point of note. What the domestic cases referenced above demonstrate is that courts are having to use very old legal instruments, such as contempt of court, to tackle new and unforeseen challenges to the judicial process and to the rights and duties of the different actors within it. If there is a regulatory gap in relation to how technological advances and new forms of social media and communication affect the judicial process, it is a gap which is not unique to this field but is instead a recurring theme across the types of cases which arise under different Convention articles discussed herein. The words of one UK practitioner in relation to social media and the Article 6 fair trial context are apposite across all the different Convention articles addressed herein:

> "New technology has weaponised language in a new way, and there is an urgent need to embrace new strategies. We need a regulator that reflects a real world understanding of how social media functions in the lives of users, and vision for an online world where free expression is balanced with the right to a fair trial. This effort must take place within a comprehensive overhaul (of) the impact of social media on the administration of justice, as we recalibrate to the realities of the 21st century."[56]

Incidentally, in conclusion, as regards judicial use of social media, the Court has held that, as a matter of principle, a judge should consider disqualifying him or herself from sitting if the judge has made public statements relating to the outcome of the case.[57] But what of a social media presence beyond a case. It is highly likely that different codes of judicial ethics now address or omit to address this subject. I won't broach here the question of judicial use of Facebook, Twitter or the like because this is a question of judicial ethics and because I might face some unfriendly audience fire. However, perhaps when it comes to judicial tweeting, one could adapt a latin phrase and say *Caveat Usor*. Our case-law to date touches on an allegation of impartiality in relation to a judge whose spouse was active on social media and in relation to a topic linked to a pending case. In *Rutsavi 2 Broadcasting Company v. Georgia*, the Court noted that, according to the Bangalore Principles of Judicial Conduct, a judge shall not allow his or her family, social or other relationships to influence his or her judicial conduct.[58] It recognised that the requirement of judicial impartiality cannot prevent a judge's family expressing their views on issues affecting society but added that it could not be excluded that the activities of close family members might, in certain circumstances, adversely affect the public's perception of a given judge's impartiality.[59]

IV - Democracy and the right to free elections and expression in a digital world

[55] In June-July 2020, the ECtHR held hearings using video-links to the parties and third party interveners.

[56] See P. Theodorou in "The impact of social media on criminal justice system - 'Ofcom of social media is welcome'" (*LNB News,* 5 March 2019) <https://www.bcl.com/wp-content/uploads/2019/03/The-impact-of-social-media-on-criminal-justice-system.pdf> accessed 11 September 2020.

[57] See, for example, *Rustavi 2 Broadcasting Company Ltd and Others v. Georgia*, no. 16812/17, 18 July 2019, §§ 341-342.

[58] See *Rutsavi*, cited above, § 344 and point 4.8 of the Bangalore Draft Code of Judicial Conduct 2001 (hereinafter "the Bangalore Principles"), adopted by the Judicial Group on Strengthening Judicial Integrity, and revised at the Round Table Meeting of Chief Justices held in The Hague in November 2002.

[59] See *Rutsavi*, cited above, § 344 and paragraph 67 of the Commentary on the Bangalore Principles.

In a remarkably short space of time new words have made their way into the democratic lexicon – fake news, junk news circulation and disinformation to name but a few. One author referred recently to "lie machines", consisting of the governments and political campaigns that produce lies alongside the social media platforms, algorithms and bots that distribute them and which attack not just specific targets but also "the liberal epistemic order, or a political system which places its trust in essential custodians of factual authority", including science, the academy, journalists, public administration and the justice system.[60] A recent Chatham House report on online disinformation and political discourse explains that disinformation in elections is part of a broader problem arising from the spread of disinformation in day-to-day online discourse:

> "[This] has encouraged tribalism and a polarization of views on a wide range of societal issues … [and t]his polarization feeds into voters' preferences in elections and into the tenor and content of political debate".[61]

Article 3 of Protocol n° 1 of our 70-year-old Convention provides that:

> "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".

Extensive case-law exists in relation to this article, covering what constitutes a legislative body, the right to vote, conditions of access for voting, the right to stand for election, the organisation of elections or election campaigns, the processing of electoral results and the resolution of electoral disputes.[62] However, what is striking is that one finds few if any references to the words digital, technology, electronic, Internet or social media in this part of the case-law. Once again, as with courts and the judicial process discussed above, the votes and elections which have been the subject of the Court's case-law thus far have been votes cast physically, perhaps by means of a postal vote, in elections organised in physical polling stations and following elections campaigns which have followed traditional lines and are subject to traditional rules, such as, for example, in some jurisdictions, a ban on campaigning in the physical vicinity of a polling booth.

The absence of case-law under Article 3 of Protocol n° 1 looking at elections and voting in a digital age is somewhat surprising, since recent elections in Council of Europe States and beyond the continent of Europe, for well-nigh a decade, have been influenced if not dominated by the use of social media, the internet and new technologies by and for voters and candidates. In a manner which mirrors the discussion of new and digital technologies from the perspectives of Articles 8 and 10, commentators both recognise the human rights benefits in the electoral sphere – a plurality of

[60] See the review of T. Rid, "The Secret History of Disinformation and Political Warfare", 2020, Farrar, Straus and Giraux, by J. Freedland, "Disinformed to Death" in *New York Review of Books*, August 2020 issue.

[61] See K. Jones, "Online Disinformation and Political Discourse. Applying a Human Rights Framework" Chatham House, The Royal Institute of International Affairs, November 2019, 8.

[62] See, for examples, in this order, *Matthews v. the United Kingdom* [GC], no. 24833/94, 18 February 1999, §§ 45-54 (on the European Parliament as a legislature); *Hirst v. the United Kingdom* (no. 2) [GC], no. 74025/01, 6 October 2005, § 62 (on the right to vote of prisoners); *Shindler v. the United Kingdom,* n° 19840/09, 7 May 2013 (justifiable restrictions on voting rights of non-resident citizens); *Sejdić and Finci v. Bosnia-Herzegovina* [GC], nos. 27996/06 and 34836/06, 22 December 2009 (rule excluding the eligibility to stand for election of persons who refused to declare affiliation with a "constituent people"); *Bowman v. the United Kingdom*, no. 141/1996/760/961, 19 February 1998, § 42 (on interaction with Article 10 and the importance in the period preceding an election for opinions and information of all kinds to be permitted to circulate freely); *Davydov v. Russia*, no. 75947/11, 30 May 2017 (on post-election periods, including the counting of votes and the recording and transmission of the results) and *Petkov and Others v. Bulgaria*, nos. 77568/01, 178/02 and 505/02, 11 June 2009 (on the need for effective remedies in electoral disputes).

voices, a new freedom of association and more widespread access to information – while also identifying the risks and, in some elections, the concrete effects of distortion to the electoral and political processes which undermine democracy and the electoral process.[63] Disinformation, fake news and the misuse of personal data, which are now features of our societies, existed before the internet and digital platforms. However, studies confirm what we all know: their reach and impact is now greater, as is their propensity to encourage tribalism and polarization.[64] Furthermore, their impact can be starkest, or more calculable, in election and referendum campaigns.

In *Magyar Kétfarkú Kutya Párt v. Hungary*, the Court got its first taste of the use of new technologies, namely a mobile phone application, in the context of an electoral campaign.[65] Although it addressed the complaint under Article 10, the electoral context and therefore aspects of its case-law on Article 3 of Protocol n° 1 of the Convention, were never far from the surface. This is hardly surprising since these rights are regarding in the Court's case-law as forming the bedrock of any democratic system.[66] The case arose in the context of a referendum held in Hungary in 2016 in relation to the EU's migration relocation plan. Just prior to the referendum the applicant political party (MKKP), which was against the referendum and whose platform encouraged the spoiling of ballots, had made available to voters a mobile application to anonymously upload and share with the public photographs of their ballot papers. The app could be downloaded through Google Play and Apple Store free of charge and it was advertised on MKKP's web and Facebook pages. Following complaints by a private individual to the National Election Commission (NEC), the applicant party was fined for infringing the principles of fairness and secrecy of elections and that of the exercise of rights in accordance with their purpose provided by Hungarian law. Handing down its second of two rulings *after* the referendum had been held, the Kúria upheld the NEC's finding regarding the infringement of the principle of the exercise of rights in accordance with their purpose, but dismissed its conclusions regarding the voting secrecy and fairness of the referendum. The applicant party's constitutional complaint was declared inadmissible.

Both the Chamber and the Grand Chamber found a violation of Article 10 of the Convention but on different grounds. The former excluded the existence of a legitimate aim, while the latter examined the case from the perspective of lawfulness under Article 10 § 2. Two forms of expressive activity were at issue: the mobile application was a means put in place by the MKKP for voters to impart their political opinions but it was also a means for MKKP to convey its own political opinion, namely spoil the ballot. In essence the Grand Chamber held that the applicant political party, in the absence of a binding provision of domestic legislation explicitly regulating the taking of ballot photographs and the uploading of those photographs in an anonymous manner to a mobile application for dissemination while voting was ongoing, knew or ought to have known – if need be, after taking appropriate legal advice – that its conduct would breach the existing electoral procedure law. The Court took no position on whether ballot photographs could or should be legalised. It's worth recalling that questions relating to ballot selfies, a different beast, have divided courts across different U.S. States for several years.[67] Instead the Court enjoined States to provide for a clear

[63] See, variously, *Jones*, cited above.
[64] Ibid, 8.
[65] *Magyar Kétfarkú Kutya Párt v. Hungary (MKKP)* [GC], no. 201/17, 20 January 2020. It should of course be noted that Article 3 of Protocol no. 1 does not apply to referenda (see, for example, *Moohan and Gillon v. the United Kingdom* (dec.), nos. 22962/15 and 23345/15, 13 June 2017.
[66] See, for example, *Mathieu-Mohin and Clerfayt v. Belgium*, no. 9267/81, 2 March 1987, § 47; *Lingens v. Austria*, no. 9815/82, 8 July 1986, §§ 41-42; and *Bowman*, cited above, § 42.
[67] The regulation of ballot selfies has been discussed in detail in the US, where it has given rise to litigation. The leading U.S. case seems to be *Rideout v. Gardner*, 838 F ; 3d 65 (1st Cir. 2016), in which the First Circuit held that a New Hampshire law prohibiting voters from

regulatory framework in their regard. The existing Hungarian legislation allowed for the restriction of voting-related expressive conduct on a case-by-case basis, thus conferring a wide discretion on electoral bodies and domestic courts called on to interpret and apply it. Indeed in this case, the Court noted that the NEC and the Kúria had disagreed as to the applicability of the basic principles of electoral procedure and while the NEC had issued guidelines to the effect that the taking of ballot photographs was in breach of domestic law,[68] those guidelines were not legally binding and their relevance and legal effects were only clarified by the Kúria *after* the referendum had taken place.[69] The electoral context was central to the Court's approach. Having reiterated that the scope of the notion of foreseeability depends to a considerable degree on the content of the instrument in question, the field it is designed to cover and the number and status of those to whom it is addressed, the Court emphasised:

> "The electoral context takes on special significance in this regard, given the importance of the integrity of the voting process in preserving the confidence of the electorate in the democratic institutions. Accordingly, the Court has found wide and unpredictable interpretations of legal provisions governing elections to be either unforeseeable in their effects or indeed arbitrary and therefore incompatible with Article 3 of Protocol No. 1 … ."

Future cases on freedom of expression in a digital age and elections are likely to put some of the basic tenets of the established case-law to the test. Take the margin of appreciation, it is narrow when the expression involved is in the context of a political debate; narrow when the work of a political party is at issue; wide when what is involved is the organisation and running of an electoral process,[70] but wide also when the issue at hand is not governed by a European consensus. The vital role of the media, as a "public watchdog" in facilitating and fostering the public's right to receive and impart information and ideas has been repeatedly recognised by the Court.[71] However, in recent case-law on the right to receive information under Article 10, the Court has held that:

> "… the function of bloggers and popular users of the social media may be also assimilated to that of "public watchdogs" in so far as the protection afforded by Article 10 is concerned."[72]

This is a major leap and one which could have important ramifications in electoral contexts as the individuals involved are not regulated as previous press public watchdogs have been. We are also likely to see more cases like *Communist Party of Russia and Others v. Russia*, in which the Court

---

sharing ballot selfies was unconstitutional under the First Amendment. The New Hampshire Code, which since 1911 had forbidden voters to show others their marked ballots, had been amended to include « this prohibition shall include taking a digital image or photograph of his or her marked ballot and distributing or sharing the image via social media or by any other means ». The statute was considered overbroad as it restricted a form of speech regardless of where, when and how that imagery was publicised. This appears to be a fundamental difference with the impugned publication at issue in the Hungarian case as the uploading and publication of the ballot photographs on the app was designed to operate in real time, when voting was ongoing, in order precisely to influence the votes of others. Another difference was of course the anonymized upload, preventing the vote and the voter to be connected.

[68] Prior to the holding of the referendum, NEC guidelines had indicated, for over two years, that taking photographs of ballot papers in the polling station constituted an infringement of the principle of proper exercise of voting rights in accordance with their purpose. The same guidelines indicated that the use of ballot papers contrary to their purpose – namely to represent the choice of voters and establish the results of voting – could also infringe the principle of the secrecy of elections. Voters were under no obligation not to divulge how they had cast their ballot, but they were under an obligation to exercise their voting rights in accordance with their purpose. Voters, according to the NEC guidelines, "cannot take the ballot paper out of the polling station and cannot take a photograph with either a telecommunication, digital or any other device with the purpose of showing it to another person".

[69] *MKKP v. Hungary*, cited above, §§ 113-114.

[70] See *Bowman*, cited above; *Ždanoka v. Latvia* [GC], no. 58278/00, 16 March 2006*; Tv Vest AS & Rogaland Pensjonistparti v. Norway*, no. 21132/05, 11 December 2008; *Orlovskaya Iskra v. Russia*, no. 42911/08, 21 February 2017.

[71] *Bladet Tromsø and Stensaas v. Norway* [GC], no. 21980/93, 20 May 1999, §§ 59 and 62.

[72] *Magyar Helsinki Bizottság v. Hungary*, no. 8030/11, 8 November 2016, § 168.

confirmed that the State has a positive obligation thereunder to ensure that coverage by regulated media was objective and compatible with the spirit of "free elections", even in the absence of direct evidence of deliberate manipulation.[73] Once again, however, the State's obligation in that case related to regulated media. There has always been an ebb and flow between the case-law on Articles 10 and 3 of Protocol n° 1 and this looks set to continue as domestic and European courts approach the internet and social media as both a vital and potentially destabilising force in public discourse and the electoral context.

V - The right to education under Article 2 of Protocol n° 1 in a digitally dependent world

Pursuant to the first sentence of Article 2 of Protocol n° 1:

> "No person shall be denied the right to education."

Article 2 of Protocol No. 1 is distinguished by its negative wording. The Contracting Parties do not recognise such a right to education as would require them to establish at their own expense, or to subsidise, education of any particular type or at any particular level.[74] There is no positive obligation for States to create a public education system or to subsidise private schools. These areas are left to their discretion. The right in this provision is one which, in the words of the Court in *Golder v. the United Kingdom*, in relation to the right of access to court, the Convention set forth without, in the narrower sense of the term, defining it. In relation to such a term, the Court has held that there is room, apart from the bounds delimiting the very content of any right, for limitations permitted by implication. In the *Belgium Linguistics* case, the Court held that:

> "The right to education ... by its very nature calls for regulation by the State, regulation which may vary in time and place *according to the needs and resources of the community and of individuals*. It goes without saying that such regulation must never injure the substance of the right to education nor conflict with other rights enshrined in the Convention."[75].

This provision thus addresses a right with a certain substance and obligations arising from it. States cannot therefore deny the right to education for the educational institutions they have chosen to set up or authorise. In addition, like all other substantive Convention articles, Article 2 of Protocol No. 1 is also closely linked to Article 14 of the Convention and to the prohibition of discrimination.

In 2011, in *Ponomaryovi v. Bulgaria*, the Court looked at the requirement for certain categories of aliens to pay secondary school fees and found, in the circumstances of the case, a violation of Articles 2 of Protocol n° 1 and 14.[76] It recognised that a State could have legitimate reasons for curtailing the use of resource-hungry public services, including education. The latter is an activity that is complex to organise and expensive to run and in regard to which the State had to strike a balance between the educational needs of those under its jurisdiction and its limited

[73] See *Communist Party of Russia and Others v. Russia*, no. 29400/05, 19 June 2012.

[74] See *Belgian Linguistic* case, Series A no. 6, p. 32. See further the Travaux préparatoires (see in particular Doc. CM/WP VI (51) 7, p. 4, and AS/JA (3) 13, p. 4). In dismissing the "positive formula" adopted by the Council of Europe Assembly in August 1950, the signatory States apparently did not want the first sentence of Article 2 of Protocol No. 1 to become interpreted as an obligation for the States to take effective measures so that individuals could receive the education of their choosing and to create education themselves, or to subsidise private education.

[75] Ibid, § 5.

[76] *Ponomaryovi v. Bulgaria*, no. 5335/05, 21 June 2011.

capacity to accommodate them. However, the Court emphasised that education is a right that enjoys direct Convention protection and is also a very particular type of public service, which not only directly benefits those using it but also serves broader societal functions and is indispensable to the furtherance of human rights. The State's margin of appreciation in this domain increases with the level of education, in inverse proportion to the importance of that education for those concerned and for society at large. Thus, at primary level, its margin is narrower. With more and more countries moving towards what had been described as a "knowledge based" society, the Court held in this Bulgarian case that secondary education plays an ever increasing role in successful personal development and in the social and professional integration of the individuals concerned. In a modern society, having no more than basic knowledge and skills constituted a barrier to successful personal and professional development and prevented those concerned from adjusting to their environment, with far reaching consequences for their social and economic well-being. Those considerations militated in favour of the Court applying stricter scrutiny to the assessment of the proportionality of the measure affecting the applicants.

As regards access to computers and internet use, the Court has held that Article 10 cannot be interpreted as imposing a general obligation to provide access to the Internet, or to specific Internet sites, for prisoners.[77] To my knowledge the Court has not yet dealt with a complaint from the general public in relation to Article 2 of Protocol n° 1. It has, however, dealt with complaints from prisoners denied computer use with Internet access to pursue their higher education studies due to the terrorist nature of the offences for which they were convicted. In *Mehmet Resit Arslan and Orhan Bingöl v. Turkey*, domestic legislation allowed convicted prisoners to continue their studies in prison to the extent of the prison's resources.[78] The Court held that access to the computers in question:

> " … constituted an indispensable material means to ensure the genuine exercise of the right to education, since it enabled the prisoners to prepare for examinations to be admitted to higher-education institutions and potentially to pursue their studies".[79]

It stressed that the manner of regulating access to audio-visual training materials, computers and the Internet fell within the Contracting State's margin of appreciation, thus recalling the proviso in *Belgian Linguistics* regarding the "needs and resources of communities and of individuals". However, the prisons in question had the means to provide their inmates with the possibility afforded by the law. Moreover, no concrete justification for the lack of resources of the prisons in question had been put forward in the domestic proceedings or before the Court. In this case, the Court held that the domestic courts had not struck a fair balance between the applicants' right to education and the imperatives of public order.

When judges refer to "blue sky thinking", they are in my view not so subtly indicating that nothing they say can or should be held against them in a court of law. They are instead merely thinking aloud, sounding out where new problems and future legal questions may lie. When handing down its 2019 judgment, the Second Section of the Court could not have envisaged that most children in Council of Europe Member States, from primary through to third level education, would be confined for months, obliged to carry on their studies in their bedrooms and around kitchen

[77] See *Kalda v. Estonia, no.* 17429/10, 19 January 2016, § 45 regarding a failure to give relevant and sufficient reasons to a prisoner for a refusing access to certain internet sites for the purpose of legal research and a violation of Article 10 of the Convention.
[78] *Mehmet Resit Arslan and Orhan Bingöl v. Turkey*, nos. 47121/06, 13988/07 and 34750/07, 18 June 2019.
[79] Ibid, § 58.

tables, as the world struggled to come to grips with its first global pandemic in a century. In the past few months, 188 countries imposed countrywide closures, affecting more than 1.5 billion children and youth.[80] Quid internet and computer access as an indispensable material means to ensure genuine exercise of the right to education in such a context? Were any such case to come before a domestic or this Court, the fair balance to be struck would inevitably have to factor in the wide margin of appreciation enjoyed by States, the question of resources, the level of education involved and questions relating to the very essence of the right to education and its effectiveness as well as alternatives means to provide for it.

VI – Conclusions

In this paper I have deliberately toured articles of the Convention which until now have been considered more peripheral in discussions of the challenges posed by technology and digitalisation to fundamental rights.

I did this in order to give a broader view of the legal challenges which have emerged or are emerging, to test how fit for purpose the case-law in relation to different Convention rights is to rise to those challenges and to highlight where the most obvious gaps in legal protection and responses may arise.

If, as I suggest, domestic law, where very often regulatory gaps are identified as problematic, and Convention law are lagging behind in relation to technological developments which have been with us for some time, ipso facto we may be unprepared for what lies ahead.

There are certainly some significant milestones and achievements in the case-law. If European data protection law is an advanced model of protection in today's digital world, one must thank the Convention, wherein lie the origins of that model. However, on the topic the subject of my presentation – technological developments and human rights – Convention law is more a work in progress than a series of fine-tuned landmark judgments to which the words milestones and achievements can be easily attached.

[80] See UN, *Policy Brief: The impact of Covid-19 on children*, 15 April 2020.