

Module 2

**Data
Protection
and Press
Freedom**

*Modules on Digital Rights
and Freedom of
Expression Online in
Europe*



ISBN 978-0-9935214-1-6

Published by Media Defence: www.mediadefence.org

This module was prepared with the assistance of ALT Advisory: <https://altadvisory.africa/>

Published in May 2024

This work is licenced under the Creative Commons Attribution-NonCommercial 4.0 International License. This means that you are free to share and adapt this work so long as you give appropriate credit, provide a link to the license, and indicate if changes were made. Any such sharing or adaptation must be for non-commercial purposes and must be made available under the same “share alike” terms. Full licence terms can be found at <http://creativecommons.org/licenses/by-ncsa/4.0/legalcode>.



TABLE OF CONTENTS

1. INTRODUCTION	1
2. THE RIGHT TO BE FORGOTTEN	3
2.1. CJEU Case-law	3
2.2. GDPR	4
2.3. Press Freedom v the Right to be Forgotten	5
2.4. 'De-indexing'	5
2.5. Anonymisation	7
2.6. Balancing in L.M. and W.W. v. Germany.....	7
2.7. The new balancing test in Hurbain v. Belgium [GC]	8
3. CONCLUSION.....	12

MODULE 2

In this new information age, the task of safeguarding personal information has gained dramatically in significance and complexity. As online data sharing and data collection continue to expand rapidly, law and policy makers play catch up with the threats the new reality poses to our privacy. Europe, with its high level of internet penetration,¹ has been at the forefront of developing legal safeguards for the protection of personal data online. Although laws and policies continue to evolve in this field and the tension between the right to personal data and other rights is far from being resolved, robust protection measures have already been implemented in most national jurisdictions and at the EU level. Some of them, however, come at a serious cost to freedom of expression. Within the Council of Europe framework, the European Court of Human Rights have tested some of these measures, with mixed results. Stronger protection of personal data is not always a bad thing for journalists. They benefit from it too, especially when it comes to such new threats as digital surveillance and online intimidation and harassment. This module, however, focuses on the aspects of data protection that come into conflict with freedom of expression online, with special emphasis the right to be forgotten.

1. INTRODUCTION

“Personal data” refers to any information relating to an identified or identifiable individual² (i.e., an individual who can be directly or indirectly identified without requiring unreasonable time, effort or resources³). While not an independent right under the European Convention of Human Rights, protection of personal data is recognised as an integral part of the right to respect for one’s private life guaranteed in **Article 8 of the ECHR**. For a long time, tension between freedom of the media and the right to privacy emerged largely from an act of *publishing* protected personal data. It is in this context that the ECtHR initially developed its approach to balancing between the two rights. However, digital technologies have revolutionised how personal data is collected, stored, analysed, and shared, and with the media having moved online, it has made almost all of media content indefinitely accessible to anyone with internet connection regardless of when it was published. Moreover, search engines have made retrieving such content exceptionally easy. In this new environment, the online *retention* of publications – that is, their continuous ready availability on the internet – has become a separate concern for anyone seeking to protect their privacy from the media. The solution to this new challenge arrived in the form of a “right to be forgotten”, famously conceptualised by the CJEU in the Google Spain case. Since then, national courts and the ECtHR have grappled with reconciling measures designed to implement the right to be forgotten with freedom of the media – with mixed results.

¹ In 2022, some 85% of Europeans were active on the internet. See Edouard Mathieu and others, ‘Number of people using the internet’ *Our World in Data* (2023) (accessible [here](#)).

² Article 2 of the Council of Europe’s Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108) (accessible [here](#)).

³ Explanatory report, para. 17 (accessible [here](#)).

Legal framework for data protection: the European Union

The right to the protection of personal data is expressly recognised in Article 8 of [the Charter of Fundamental Rights of the European Union](#) (which is binding on both the EU institutions and bodies and the EU member states). Article 8 stipulates that personal data “must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law” and that everyone “has the right of access to data which has been collected concerning him or her, and the right to have it rectified.” It also obliges member states to establish independent authorities to supervise the implementation of these requirements.

Central to the EU’s data protection regime is the [General Data Protection Regulation](#) (GDPR), adopted in April 2016. As the world’s most advanced piece of legislation on the subject, it has influenced data protection laws in many countries outside the EU.

The **GDPR’s regime is based on the following principles** for processing personal data:⁴

- Personal data must be processed fairly and lawfully, and must not be processed unless the stipulated conditions are met.
- Personal data must be obtained for a specified purpose (or purposes), and must not be further processed in any manner incompatible with that purpose.
- Personal data must be adequate, relevant and not excessive in relation to the purpose (or purposes) for which it is processed.
- Data must be accurate and, where necessary, kept up to date.
- Personal data must not be kept for longer than is necessary for collection.
- Personal data must be processed in accordance with the rights of data subjects provided for under the data protection law.
- Appropriate technical and organisational measures must be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.
- Personal data must not be transferred to another country that does not ensure an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal information.

Legal framework for data protection: the Council of Europe

The 1981 [Convention for the Protection of Individuals with regard to Automated Processing of Personal Data](#) (a.k.a. Convention 108) was the first legally binding international instrument dedicated to data protection. In 1999, it was [amended](#) to allow the European Communities to join it. In 2001, an [Additional Protocol](#) was adopted to introduce new obligations related to supervisory authorities and transborder data flow. Finally, in May 2018, an [Amending Protocol](#) was adopted to introduce a new, “modernised” version of the Convention, referred to as [Convention 108+](#) (not yet in force).⁵ The modernisation version brings the Convention closer to the GPDR regime. However, one of the significant remaining gaps is that Convention 108+

⁴ Information Commissioner’s Office, ‘A guide to the data protection principles’ (accessible [here](#)).

⁵ For a summary of the main changes introduced by Convention 108+, see Council of Europe, ‘The modernised Convention 108: novelties in a nutshell’ (accessible [here](#)).

does not introduce a data subject's right to obtain the erasure of their personal data (the right to be forgotten), which is expressly guaranteed in Article 17 of the GDPR.

In addition, the Committee of Ministers of the Council Europe has adopted several recommendations directly relevant to data protection online:

- Recommendation [CM/Rec\(2010\)13](#) of the Committee of Ministers to member States on the protection of individuals with regard to automatic processing of personal data in the context of profiling;
- Recommendation [CM/Rec\(2012\)3](#) of the Committee of Ministers to member States on the protection of human rights with regard to search engines;
- Recommendation [CM/Rec\(2012\)4](#) of the Committee of Ministers to member States on the protection of human rights with regard to social networking services.

As was mentioned above, the right to the protection of one's personal data has been read by the European Court of Human Rights into Article 8 of the ECHR. A few examples of the large variety of personal data the European Court of Human Rights ('the ECtHR') has found to be protected by Article 8 include: internet subscriber information associated with specific dynamic; fingerprints, cellular samples, and DNA profiles; publicly accessible information on the taxable income and assets of private individuals; data collected by means of non-covert video surveillance.⁶

2. THE RIGHT TO BE FORGOTTEN

Digital technologies have fundamental changed not only how media content is created and published, but also how it can be stored, shared and accessed. Thanks to search engines, an article published online can now be easily retrieved by anyone with internet connection – and, in theory, may continue to be so for an indefinite period. This is even increasingly true for old publications that first existed only in print form, as print media archives become digitalised and available online.

The continuous ready availability of media content on the internet has become a separate data protection concern, the regulative response to which has taken the form of a "right to be forgotten."

2.1. CJEU Case-law

The right to be forgotten was famously endorsed by the Court of Justice of the European Union in the [Google Spain](#) case in 2014. At the heart of that case was a complaint to the Spanish Data Protection Agency that had been submitted by a person who did not want for two old newspaper reports with his name in them to appear in Google search results when his name was entered in the search engine. The part of the complaint that related to the newspaper had been rejected by the agency (as it found the publication of the information to be legally justified). However, the agency had upheld the request that Google remove links to the articles

⁶ For more examples, see ECtHR's Guide to the Case-Law of the of the European Court of Human Rights guide, p. 8 (accessible [here](#)).

from its search results. Google challenged the decision in Spanish courts, which eventually led to the case's referral to the CJEU for a preliminary ruling.

The CJEU established that a search engine was a 'controller' in the meaning of EU data protection law (paras.33-34) and the very display of personal information on a search results page constituted processing of that data (para. 57). It then observed that the processing of personal data by a search engine "is liable to affect significantly the fundamental rights to privacy and to the protection of personal data when the search [...] is carried out on the basis of an individual's name, since that processing enables any internet user to obtain through the list of results a structured overview of the information relating to that individual that can be found on the internet — information which potentially concerns a vast number of aspects of his private life and which, without the search engine, could not have been interconnected or could have been only with great difficulty — and thereby to establish a more or less detailed profile of him" (para. 80). The impact on the rights of data subjects is magnified by "the important role played by the internet and search engines in modern society, which render the information contained in such a list of results ubiquitous" (ibid). At the same time, the CJEU recognised that de-listing of links from search results could affect internet users' legitimate interest in access information and, therefore, requires balancing that takes account of the nature of the information in question, its sensitivity for the data subject's private life, and the interest of the public in having that information (para. 81).

The CJEU concluded that data subjects' requests for delisting lawfully published and factually accurate content must be satisfied, if the information "appears, having regard to all the circumstances of the case, to be inadequate, irrelevant or no longer relevant, or excessive in relation to the purposes of the processing at issue carried out by the operator of the search engine" (para. 94). However, an exception would have to be made when "for particular reasons, such as the role played by the data subject in public life, that the interference with his fundamental rights is justified by the preponderant interest of the general public in having, on account of inclusion in the list of results, access to the information in question" (para. 97).

The **de-listing obligations** of search engines was further refined in several subsequent cases. In particular, in [GC and Others](#), the CJEU clarified the responsibilities of search engines in respect of so-called sensitive data (this type of data is defined in Article 9 of the GDPR which, with certain exceptions, prohibits its processing). The CJEU concluded that because of how search engines operate the restrictions on processing sensitive data do apply to them *ex ante* and systematically. Instead, search engines are only obliged to conduct *ex post* verification at the request of a data subject (para. 47). Other relevant cases include [Google v CNIL](#) (the territorial scope of the right to be forgotten) and [TU, RE v Google LLC](#) (delisting inaccurate information).

2.2. GDPR

Following the CJEU ruling in *Google Spain*, the right to erasure/the right to be forgotten was expressly introduced by the GDPR in Article 17. The right applies in the following circumstances:

- When the personal data is no longer necessary for the purpose for which it was originally collected or processed;

- When the data controller is relying on an individual's consent as the lawful basis for processing the data and that individual withdraws their consent;
- When the data controller relies on legitimate interests as its justification for processing an individual's data, the individual objects to this processing, and there is no overriding legitimate interest for the data controller to continue with the processing;
- If a data controller is processing personal data for direct marketing purposes and the individual objects to this processing;
- If a data controller processed an individual's personal data unlawfully;
- If personal data must be erased in order to comply with a legal obligation; or
- A data controller has processed a child's personal data in order to offer access to information society services.⁷

Importantly, **Article 17 also provides for exceptions** to the right to erasure which include, in particular, data processing necessary for exercising freedom of expression and information and for archiving purposes in the public interest or scientific or historical research.

The European Data Protection Board has issued [guidelines](#) on the application of Article 17 to search engines.

2.3. *Press Freedom v the Right to be Forgotten*

The CJEU case-law discussed above has dealt with only one of the possible ways to realise the right to be forgotten, namely, delisting through the removal of a link from search results based on the name of the person concerned. However, **national jurisdictions have developed other measures**, including those aimed directly at publishers/content providers. They include requesting website publishers to:

- de-index the article fully or partially by means of access codes or directives issued to search engine operators, so as to prevent certain publications to appear in name-based search results;
- remove a certain article from the index of the website's internal search engine;
- add a note to a published text where the information it contains is inaccurate, incomplete or outdated;
- anonymise the person referred to in the contested text;
- remove all or part of the contested text from a digital archive.

While the negative impact of search engine delisting on freedom of the media should not be underestimated, the impact of obligations imposed directly on publishers is, arguably, even more serious. The ECtHR has tested some of these measures, as it grapples with finding the right balance between the right to privacy manifesting itself in the right to be forgotten, on the one hand, and freedom of expression, on the other.

2.4. *'De-indexing'*

Similarly to delisting by search engines, 'de-indexing' – in the sense this term has been used by the ECtHR – is designed to make it impossible to search for an article about a certain

⁷ GDPR.EU, 'Everything you need to know about the "Right to be forgotten"' (accessible [here](#)).

person by entering the name of that person into a search tool, without affecting the article's content or online location. De-indexing, however, is carried out not by search engines, but by publishers/ website owners.

In *Biancardi v. Italy* (appl. no. 77419/16, judgment of 25 November 2021), the ECtHR examined the compatibility of de-indexing with freedom of expression for the first time. The applicant was the editor-in-chief of an online newspaper that had been required to de-index an old article about a restaurant fight and the resultant criminal case. About two and a half years after the publication, one of the persons involved in the fight requested that the applicant remove the article from the internet. The applicant refused to do it, but eight months later he de-indexed the article in an attempt to settle the court case initiated by the requestors. The domestic courts, however, found the applicant liable for failing to have the article de-indexed in a timely manner and ordered him to pay moral damages to the plaintiff. At the same time, the courts were satisfied that de-indexing alone was sufficient (as opposed to removing the article). The ECtHR agreed with the domestic courts and found that the applicant's freedom of expression had not been violated.

Most of the Court's previous balancing between freedom of expression and the right to privacy was concerned with the lawfulness of initial publications. In this case, however, it was the continued availability of an initially lawful publication that had to be assessed. This crucial difference led the Court to begin adapting its balancing exercise to the right to be forgotten. The Court identified the following two aspects of the case as the most relevant: the period for which the article remained online and how it impacted the right of the person concerned to his reputation, and the fact that the data subject was a private individual not acting within a public context as a political or public figure (para. 62).

In *Biancardi*, the Court effectively set aside the criteria formulated by the Grand Chamber in *Axel Springer AG v. Germany* [GC] (appl. no. 39954/08, judgment of 7 February 2012) (see para. 64). Instead, it focused on the following:

- (i) **the length of time for which the article was kept online:**
The criminal proceedings against the requesting party were still underway at the time the final decision was made by the Italian courts in the applicant's case. However, the Court did not make much of this fact, pointing out instead that the information contained in the article had not been updated since the occurrence of the events described (para 65). The Court also found it relevant that the article remained easily accessible (searchable) for eight more months after the formal right-to-be-forgotten request was submitted to the applicant (ibid).
- (ii) **the sensitiveness of the data:**
Because the data included in the article related to criminal proceedings, the Court considered it as 'sensitive' (and, presumably, requiring a higher level of protection) (see para. 67).
- (iii) **the gravity of the sanction imposed on the applicant (see para 64):**
The applicant was held liable under civil law (as opposed to criminal law), and while the amount of compensation he was ordered to pay was "not negligible", the Court did not find it to be excessive (para 68).

It is important to mention that in its Grand Chamber judgment in *Hurbain v. Belgium* (discussed below), the Court again revised the balancing test for right-to-be-forgotten cases, incorporating both the Biancardi criteria and the criteria previously articulated in *Axel Springer AG v. Germany*.

2.5. Anonymisation

With digitalised press archives made widely accessible online, it became conceivable for initially lawful publications to grow incompatible with the right to privacy simply because after a certain time the information they contained has lost its relevance. The ECtHR first grappled with this possibility in *L.M. and W.W. v. Germany* (appl. nos. 60798/10 and 65599/10, judgment of 28 June 2018). The applicants sought the anonymisation of old media files related to their criminal trial which, fourteen years later, were still available online. While recognising the novelty of the legal issues raised by the case, the Court applied the same balancing criteria as those developed for dealing with initial publications. It agreed with the decision of the German Federal Court of Justice to reject the applicants' request. In its Grand Chamber judgment in *Hurbain v. Belgium* [GC] (appl. no. 57292/16, judgment of 4 July 2023), the ECtHR revisited the issue of anonymisation, recalibrating the balancing test and, controversially, endorsing the modification of the contents of an initially lawful publication as an alternative to having it delisted or de-indexed.

2.6. Balancing in *L.M. and W.W. v. Germany*

L.M. and W.W. v. Germany

In 1993, the applicants were convicted of the murder of a well-known actor and sentenced to life imprisonment. In 2007, as they were about to be released from prison, they initiated proceedings against several media organisations, seeking the anonymisation of certain archive files related to the 1993 trial documents as they were still accessible on the organisations' websites. Their anonymisation requests were eventually rejected by the Federal Court of Justice.

Although the relevant media materials were unquestionably lawful at the time of their publication, the ECtHR recognised that the applicants had a legitimate Article 8 interest "in no longer being confronted with their acts, with a view to their reintegration" (para. 100). It tacitly accepted that the right to be forgotten could, in principle, impose obligations on the original publisher of information containing protected personal data. However, it indicated that the balancing outcomes might be different for a publisher ("whose activity is generally at the heart of what freedom of expression is intended to protect") and a search engine ("whose main interest is not in publishing the initial information about the person concerned, but in particular in facilitating identification of any available information on that person and establishing a profile of him or her") (para. 97). In other words, the Court suggested that a person's right to have certain media content delisted by search engines did not automatically translate into their right to have that content modified (anonymised).

For the actual balancing, the Court applied the same criteria as those it previously adopted for dealing with the privacy impact of media content at the time of its publication. In reaching its conclusion that the continuing online availability of the relevant media materials did not violate the applicant's rights under Article 8, the Court considered the following points:

(i) The materials' continuing contribution to a debate of public interest

The Court recognised that the public had an interest "in being informed about criminal proceedings and in being able to obtain information in that regard, especially when the proceedings concern particularly serious judicial facts which attracted considerable attention" (para. 98). Crucially, the contested materials still retained their public interest value when the anonymisation requests were made (para. 105).

The Court also recognised that anonymising a media report was still a sufficiently serious interference with freedom of the media, even if it was less restrictive than the deletion of the report in its entirety. Having reiterated that "the approach to covering a given subject was a matter of journalistic freedom", it concluded that "the inclusion in a report of individualised information such as the full name of the person concerned [was] an important aspect of the press's work [...], especially when reporting on criminal proceedings that have attracted considerable interest" (para. 105).

(ii) The applicants' public profile

The Court concluded that the applicants were not simply private individuals unknown to the public at the time of their request for anonymity. They acquired a degree of notoriety during the trial, which attracted considerable public attention because of the nature of the crime and the fame of the victim. Although the public's interest in the crime began to wane with time, the applicants returned to the limelight when they made several attempts to have their case reopened and spoke to the press on the matter (see para. 106).

(iii) The applicants' prior conduct vis-à-vis the media

The applicants' courted media attention as they campaigned for having their case reopened (see para. 108).

(iv) The materials' content, form, and dissemination

The contested materials reported objectively on the trial and their veracity, and their lawfulness at no time of publication was not called into question (para. 111). They only appeared in sections of the relevant websites that were clearly labelled as old news coverage, and, for that reason, they were not likely to attract the attention of internet users who were not seeking information about the applicants (paras. 112 and 113). There was no indication that access to the reports was maintained with the intention of re-disseminating information about the applicants (para. 113).

Although the Court expressly refrained from considering less restrictive alternatives to anonymisation because this point had not been discussed by the domestic courts, it did observe that the applicants had made no attempt to contact search engine operators to make the contested reports less easy to find (para 114).

2.7. The new balancing test in *Hurbain v. Belgium* [GC]

In this Grand Chamber [judgment](#), the ECtHR revisited the issue of anonymisation, refining and expanding the criteria for balancing freedom of the media against the right to be forgotten. The applicant, a newspaper publisher, was ordered by a Belgian court to anonymise the online version a twenty-year-old article stored in the newspaper's digital archive. The article contained a report on a fatal traffic accident and included the full name of the person responsible. The anonymisation order was based on a right to be forgotten request made by that person.

The Grand Chamber found the anonymisation order to be justified and, therefore, not in violation of the applicant's right to freedom of expression. It was the factual difference between this case and the one discussed above – especially, the difference in the public interest value of the respective publications and the respective profiles of the persons seeking the anonymisation – that ultimately accounted for a different balancing outcome. However, the Court also formulated additional balancing criteria, creating a test specific to the right to be forgotten.

As the Court was at pains to emphasise, the article was originally published in a lawful and non-defamatory manner, and the case concerned solely its continued availability of the information on the internet (see para. 134). Having stressed the “secondary but nonetheless valuable role” of the press in maintaining publicly available news archives (para 140), the Court declared the integrity of digital press archives to be “the guiding principle underlying the examination of any request for the removal or alteration of all or part of an archived article which contributes to the preservation of memory, especially if, as in the present case, the lawfulness of the article has never been called into question” (para. 145).

It is not clear, however, if this recognition of the importance of digital press archives had any meaningful effect on the actual balancing conducted by the Court and, particularly, on its examination of less restrictive alternatives such as de-indexing.

The balancing test included the following points:

(i) The nature of the archived information:

The inclusion of a person's full name in a press report on criminal proceedings against them did not, as such, raise an issue under the Convention, even though that information fell within the personal sphere protected by Article 8 (para. 216). The Court was satisfied that the article under consideration reported the accident accurately, succinctly, and objectively (para 219). At the same time, the reported events did not belong to “the category of offences whose significance, owing to their seriousness, is unaltered by the passage of time”; nor did they attract widespread publicity at the time or at a later point (para 219).

(ii) The time passed since the events and their initial reporting:

The Court began with a somewhat tautological observation that “the relevance of information is often closely linked to its topicality” (para. 220). Here, however, the Court's actual focus was not on the lasting relevance of the article's contents (this aspect was examined under the next criterion). Instead, the Court turned to the interests of the person requesting the anonymisation: “the passage of a significant length of time has an impact on the question whether a person should have a ‘right to be forgotten’” (ibid).

Given that sixteen years had passed between the initial publication and the anonymisation request, the Court concluded that the person in question (who had been rehabilitated in the meantime) “had a legitimate interest, after all that time, in seeking to be allowed to reintegrate into society without being permanently reminded of his past” (para. 221).

(iii) The contemporary interest of the information

The question here was whether, at the time of the submission of the anonymisation request, the article continued contributing to a debate of public interest or presented “any historical, research-related or statistical interest” (para. 222). While the existence of contemporary public interest in the information included in the article would have left “little scope” for exercising the right to be forgotten (para. 223), its absence was not necessarily decisive as long as the information could still be of interest for historical or scientific purposes (para. 224). The Court found that none of those elements were present in this case. It sided with the domestic courts’ conclusion that: (a) the article “merely made a statistical contribution to a public debate on road safety”, (b) the identity of the person responsible for the accident did not add to the article’s public interest as he was not a public figure, and (c) the reported events were “unexceptional” and “clearly not of historical significance” (see para. 224).

This approach is not easily reconciled with the importance of press archives the Court recognised earlier in the judgment. The dissenting opinion offered a compelling rebuttal to the majority’s position:

Taking into account the characteristic role of press archives, which is to preserve information, the effects of the passage of time should not be accorded too much weight in determining whether an article in the archives may be altered. Information published about a past event, which is initially relevant only as recent news concerning a person not in the public eye, may subsequently become more relevant if the person concerned comes to the forefront of public attention. Furthermore, archived information may have acquired historical, research-related or statistical interest or continue to have value for the purposes of placing recent events in context ...” (para. 11).

(iv) The public profile of the person requesting the anonymisation:

The person in question was unknown to the public either at the time of the reported events or at the time of his request, and the case did not attract widespread publicity at any point (para 229).

(v) The personal impact of the continuing availability of the information online:

As a general rule, “an attack on a person’s reputation must attain a certain level of seriousness and be made in a manner causing prejudice to personal enjoyment of the right to respect for private life” (para 231). In contrast to delisting requests addressed to search engines, the existence of “serious harm” was required for anonymisation requests that directly interfere with archived content (see para 232). In the case of a publication containing judicial information, the mere fact the person seeking anonymisation has been rehabilitated is not sufficient to justify their claim (para 233).

The Court agreed with the Belgian court’s conclusion that the information about his criminal conviction was “readily accessible to a wide audience which – since [the anonymisation requestor] was a doctor – inevitably included patients, colleagues and

acquaintances, and was thus liable to stigmatise him, seriously damage his reputation and prevent him from reintegrating into society normally” (paras. 234-235).

(vi) The degree of accessibility of the archived article:

The Court observed that an article stored in a digital archive was not likely to attract the attention of internet users who were not looking for information about a specific person (para 237). Nonetheless, the decisive consideration was whether access to an archived article was unrestricted or limited to subscribers or in some other way (para 238). In this case, public access to the digital archive was free of charge and unrestricted (para. 239).

(vii) The impact of anonymisation on freedom of expression/ freedom of the press:

The Court started by outlining various measures that have been developed in national jurisdictions to implement the right to be forgotten (see para. 241). Some are aimed at search engines (adjustments to how search results are presented; complete or partial delisting for searches based on the name of the person concerned). Others are aimed directly at website publishers and so, presumably, amount to a more serious restriction on freedom of expression (having the article de-indexed by search engines or de-indexing it on the publisher’s own website; adding a note to the original text; anonymising; removing all or part of the text from the digital archive).

The Court then went on to introduce a specific proportionality test that national courts are required to apply when examining the appropriateness of a specific measure: national courts “must give preference to the measure that is both best suited to the aim pursued by [the requesting person] – assuming that aim to be justified – and least restrictive of the press freedom which may be relied on by the publisher concerned” (para. 242).

It is important to note that the Court limited the requirement to consider less restrictive solutions to considering only measures aimed at the publisher and not those aimed at search engines, signalling this limited approach earlier in the judgment, when it stated that “the examination of an action against the publisher of a news website cannot be made contingent on a prior request for delisting” (para. 168). As a result, the Court confined itself to comparing anonymisation (“a particular means of altering archived material in that it concerns only the first name and surname of the person concerned”) to more radical interferences with the original content, such as the removal of an entire article (para. 249). As an additional justification for the choice of anonymisation, the Court referred to the fact that the original non-anonymised version of the article would still be available in print form and could be consulted by any interested person, thereby “fulfilling its inherent role as an archive record” (para. 252).

The Court’s refusal to consider delisting as a less restrictive solution contradicted its own acknowledgment that “G.’s chief concern was the fact that the article was displayed following Internet searches based on his first name and surname carried out via search engines” (para. 244). Nor does it sit well with the Court’s declaration that the integrity of digital press archives should its guiding principle. Unsurprisingly, the majority’s failure to consider delisting as a less restrictive measure that would serve the requesting person’s aims was one of the main criticisms Judge Ranzoni levelled against the judgment in his

dissenting opinion, joined by four other judges (see paras. 21-26 of the dissenting opinion).

The Court's position on the chilling effect of anonymisation is also vulnerable to criticism. Rather than considering the potential long-term effect on the media in general, it limited itself to addressing the more immediate impact of the anonymisation order on the applicant's newspaper only. In this regard, the Court noted that "in the circumstances of the present case, it [did] not appear from the file that the anonymisation order had [had] such a profound impact on the performance by the newspaper *Le Soir* of its journalistic tasks as to impair that performance in practice" (para 254). The dissenting opinion compellingly criticised the majority for its failure to address this vital question in a meaningful way, noting that "an obligation to review at a later stage the lawfulness of keeping an article online following [a right to be forgotten request] entails the risk, *inter alia*, that the press may refrain in future from keeping reports in its online archives or that it will omit individualised elements in articles that are likely to be the subject of such a request at a later stage" (para 27).

3. CONCLUSION

Establishing the limits of data protection vis-à-vis freedom of expression remains to be a work in progress for lawmakers and courts. This module has provided some insights into the complexity inherent in the task.

Europe has developed two parallel but interdependent and mutually enriching data protection regimes: within the EU and in the framework of the Council of Europe. The GDPR is at the centre of the EU regime, and its influence has spread far beyond the EU borders. The right to be forgotten, endorsed by the CJEU and later entrenched in Article 17 of the GDPR, is among the elements of the EU data protection law that have a particularly profound effect on the freedom of the media.

The EU has been an undisputed world leader in developing regulatory responses to the new threats digital technologies pose to the right to privacy. However, their impact on freedom of the media is a serious concern. The ECtHR has tested some of those responses, and its approach to balancing the right to be forgotten against freedom of expression has become more sophisticated and nuanced. Yet, one may question if the chilling effect of measures such as retroactive anonymisation is fully appreciated by the Court.