5
Prohibition of General Monitoring Obligations

5.1 Introduction

The general monitoring obligations prohibition (GMOP) is an important principle of European Union (EU) digital services regulation. It protects *content creators* and *gatekeepers* of user-generated content, similar to how media privileges[1] protect *journalists* and *news organisations* when they publish editorial content. It limits what can be expected from regulatory enforcement by stipulating that relevant providers should not be required to take excessive and indiscriminate actions that could legitimately affect all content creators. The GMOP acts as an ordering principle for national and EU legislation on digital services by distributing responsibility in the digital ecosystem. Over the years, the GMOP has obtained 'quasi-constitutional' status because it started serving as a legislative and human-rights ceiling on digital regulation.

Originally, the GMOP was mainly intended to double down on the policy rationale behind the liability exemptions.[2] The knowledge-based exemptions cannot logically function if there is a concurrent obligation to obtain knowledge.[3] Liability exemptions incorporate the idea that the responsibility for correcting wrongdoing in the digital ecosystem ought to be *shared* between different participants. It should primarily fall on content creators themselves and only secondarily on victims and providers or state authorities and civil society.

[1] See Damian Tambini, 'What is Journalism? The Paradox of Media Privilege' (2021) 5 European Human Rights Law Review 523, 537: 'Journalism is made possible by a variety of privileges and protections for both the activities of public interest newsgathering and the status of journalism.'

[2] The European law owes its existence to s 512(m) United States (US) Digital Millennium Copyright Act (DMCA). See s 512(m) DMCA: 'Nothing in this section shall be construed to condition the applicability of subsections (a) through (d) on—(1) a service provider monitoring its service or affirmatively seeking facts indicating infringing activity, except to the extent consistent with a standard technical measure complying with the provisions of subsection (i); or (2) a service provider gaining access to, removing, or disabling access to material in cases in which such conduct is prohibited by law.'

[3] Case C-18/18 *Eva Glawischnig-Piesczek v Facebook Ireland Limited* ECLI:EU:C:2019:458, Opinion of AG Szpunar, paras 36, 41.

The GMOP forms the central part of the *digital social contract*. Under this digital social contract, victims of illegal content (or someone acting on their behalf) assist in finding and notifying illegal content, and the providers are usually expected to act upon the received notifications or court orders if they wish to be exempted from liability. The underlying logic is the following: imposing an obligation on providers to constantly vet user content would push them to become editorial media, thus reducing the instances where all content is user-generated. Crucially, the GMOP prohibits the Member States from legislating obligations that would significantly reverse the baseline distribution of tasks as outlined in the liability exemptions. For instance, legislation requiring providers to review 10% of the uploaded content manually would violate the GMOP because it reverses the baseline distribution of liability.

Only the EU itself can modify this digital social contract for European citizens. That said, even the EU legislature must consider the fundamental rights constraints discussed in Chapter 3. These constraints do not allow legislatures to make far-reaching changes from the red lines drawn by the Court of Justice of the European Union (CJEU).

Prior to Article 8 Digital Services Act (DSA), its predecessor, Article 15(1) E-Commerce Directive (ECD), provided that:

> Member States shall not impose a general obligation on providers, when providing the services covered by [one of the liability exemptions], to monitor the information which they transmit or store, nor a general obligation actively to seek facts or circumstances indicating illegal activity.

Article 15(2) ECD reassured that the previous prohibition did not limit the possibility of Member States imposing notification, communication, or disclosure duties where they might be required from such providers. Recital 47 ECD clarified that Article 15 ECD does not stand in the way of 'specific' monitoring.

Back in 2000, when ECD was adopted, the GMOP followed a double objective: on the one hand, it intended to harmonise diverging national rules, and on the other hand, it aimed to protect an incipient industry from burdensome or impossible obligations which would stifle market entry. The ECD explained that: 'both existing and emerging disparities in Member States' legislation and case law concerning the liability of service providers acting as intermediaries prevent the smooth functioning of the internal market, in particular by impairing the development of cross-border services and producing distortions of competition …'.[4] The prohibition of general monitoring obligations was understood as the other side of the coin of liability exemptions. The drafters argued that the liability exemption would have been deprived of any effect if providers could be obliged by the Member States to identify illegal items at the source anyway.[5] Without the GMOP, for instance, the limitation that liability can be imposed only upon

[4] European Parliament and Council Directive 2000/31/EC of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market [2000] OJ L178/1 (ECD), Rec 40.

[5] Emmanuel Crabit, 'La Directive Sur Le Commerce Électronique. Le Projet "Méditerranée"' (2000) 4 Revue du Droit de l'Union Européenne 749, 815.

actual knowledge could have been circumvented by imposing non-monetary obligations to review everything uploaded to the services indiscriminately and manually. Furthermore, it would have been impossible for providers to avail themselves of the liability exemption dependent on a lack of knowledge if they had a concurrent obligation to know. Without the GMOP, the liability limitations would have a huge blind spot.

While ECD had a strong economic angle, it did not entirely ignore the liability exemptions' role in the context of fundamental rights.[6] The CJEU quickly linked the GMOP in Article 15 ECD to the fundamental rights protection of users by highlighting the need to protect them from interference by private and public actors. This close link was identified early on,[7] and it was strengthened in the recent case law of the CJEU, giving this provision a quasi-constitutional position; that is, a position that allows the legislature to slightly move behind its statutory red lines, but also not too far.

While the GMOP remains central to digital regulation, precisely what it entails is disputed. Article 8 DSA is the only provision in the Commission's proposal for the DSA that was not subject to any *substantive* change by the co-legislators—even though the issue was extensively debated. Some stakeholders tried to water down the language used in the ECD; others attempted to strengthen it. The tussle resulted in no material change for the provision. This demonstrates that everyone eventually felt that if they could not bend the provision their way, sticking with the Court's interpretation was the preferable way forward.

5.2 Scope of the GMOP

The last two decades since the adoption of the ECD led to seven CJEU cases dealing with the GMOP provision.[8] The GMOP in Article 15 ECD often played a very important role in defining the outcomes, sometimes in unexpected ways. Given this central role, it is perhaps a little surprising that the actual contours of the provision remain largely disputed to this day. While the consensus around the wording of the DSA renewed the democratic mandate of the GMOP, the divergence of views on interpreting this provision will continue to exist. Stakeholders mostly agree on it 'in principle', but their exact views differ.

To identify what the GMOP means, it is necessary to clarify what an 'obligation' means, which qualifies as 'monitoring' (or 'fact-finding') and when it is 'general'.

[6] ECD, Rec 46.

[7] Case C-324/09 *L'Oréal SA and Others v eBay International AG and Others* ECLI:EU:C:2011:474 (*eBay*), para 139 ('… a general monitoring obligation would be incompatible with Article 3 of Directive 2004/48, which states that the measures referred to by the directive must be fair and proportionate and must not be excessively costly'). It was addressed more explicitly in *SABAM* and *Scarlet Extended*, see Case C-360/10 *SABAM v Netlog NV* ECLI:EU:C:2012:85 (*SABAM*) and Case C-70/10 *Scarlet Extended SA v SABAM* ECLI:EU:C:2011:771 (*Scarlet Extended*). In *Glawischnig*, the AG explicitly highlighted the link, although the court does not mention this, see Case C-18/18 *Eva Glawischnig-Piesczek v Facebook Ireland Limited* ECLI:EU:C:2019:821.

[8] *eBay* (n 7); *Scarlet Extended* (n 7); *SABAM* (n 7); Case C-314/12 *UPC Telekabel Wien GmbH v Constantin Film Verleih GmbH* ECLI:EU:C:2014:192; Case C-484/14 *Tobias McFadden v Sony Music Entertainment Germany GmbH* ECLI:EU:C:2016:689; *Glawischnig* (n 7); Case C-401/19 *Republic of Poland v European Parliament and Council of the European Union* ECLI:EU:C:2022:297.

5.2.1 What is an 'obligation'?

The GMOP covers every type of obligation. Thus, it covers any measure of the state, be it of the judiciary, legislature, or executive. The obligation can be a decision in an individual case, such as an order or generally worded legislation. The crucial element is that the Member States and the respective EU bodies give those obligations some authority. In contrast, political demands communicated in the media without a proper legal basis are unlikely to qualify as obligations. Understandably, there is a large grey zone of political coercion when enforcement authorities might ask providers to 'do more' by means of 'voluntary measures'. The GMOP, in my view, limits any threats by authorities that have some legal credibility, ie those that are at least arguably enforceable. Thus, an authority of a Member State regulating digital content and demanding what amounts to general monitoring would violate Article 8 DSA, but a Member of the European or national parliament demanding the same would not.

Typical obligations imposed by *authorities* are legal orders issued by administrative authorities, criminal courts, or civil courts. The types of measures can range from website blocking, blocking of accounts, payments, freezing user privileges, removing or disabling content, delisting search results, preventing the reappearance of some content or recurrence of some conduct, limiting access to some services, or storing some data about third parties. Typical obligations imposed by *legislatures* are legal mandates to block accounts, remove or disable content, prevent the reappearance of content or recurrence of conduct, store data about third parties, or best efforts types of obligations to perform various checks. Compared to the situation before the DSA, many potential obligations of this kind are now harmonised by the DSA's due diligence obligations. Pre-emption can also come from other parts of the DSA (Chapter 17).

Given that the change of wording introduces a passive form ('no general obligation to monitor … shall be imposed'), one open question is to what extent the principle binds non-state actors or limits public-private arrangements. The CJEU will undoubtedly have to clarify this. Two basic constellations are possible: first, an obligation is *imposed unilaterally* (eg an app store imposes it on its clients, the apps), or second, an obligation is *individually negotiated* (eg providers and interested non-governmental organisations (NGOs) agree on it in their fully negotiated contracts). In my view, given that only *voluntary* general monitoring is permitted, using contractual freedom to negotiate and solidify the same measures individually should be equally possible. Those measures are not subject to Article 8 DSA. On the other hand, Article 8 DSA should prevent any 'obligations' that are 'non-voluntary'. Recital 26 reminds us that '[v]oluntary actions should not be used to circumvent the obligations of providers of intermediary services under this Regulation'. Thus, for instance, if an app store implements general monitoring in its capacity as a very large online platform (VLOP) trying to satisfy the DSA's risk management obligations, the resulting obligations imposed on app developers are not voluntary. They originate from the legal mandate the app store internalises in response to Article 34 DSA.

5.2.2 What is 'monitoring'?

From the reported history behind the ECD, it is evident that Article 15 ECD was intended to cover measures ranging from broad filtering of hosted information to area obligations, such as those adopted to protect minors.[9] The term covers all kinds of general measures, including those that did not request monitoring by name but have the same effect.[10] For instance, an abstract obligation 'to protect minors' can mean the creation of tools for parents but also an obligation to observe and evaluate users to assess their age. Only the latter obligation would qualify as monitoring. In the context of the DSA, this 'by object or effect' distinction is now also reflected in the words of 'de jure or de facto' in Recital 30 DSA. The European Parliament demanded clarification during the negotiations.

The GMOP has two prongs: a) monitoring the information stored or transmitted, and b) actively seeking facts or circumstances indicating illegal activity. The CJEU case law to date is silent on the difference. Fact-finding seems to imply obligations involving human judgement while monitoring mostly implies using machines.[11] Fact-finding implies discovering, acquiring, and establishing facts by someone. Monitoring, in contrast, customarily means an act of observing or recording. It thus implies surveillance over someone or something by either people or machines. Taken together, monitoring practically means surveillance of users and their content on the digital service.

When a measure targets past actions or static targets, such as removing specific illegal content on a URL, there is usually very little concern that this would amount to 'monitoring'. In such cases, the content can be identified with precision using a URL or an Internet Protocol (IP) address and domain name. To comply, the provider does not usually have to monitor anything. It simply removes specific content, blocks accounts, or deregisters a domain name. In contrast, the greatest difficulty comes with measures that attempt to police *future lawless acts* or *moving targets* on a particular service.[12] In order to fulfil such orders, providers must usually 'monitor the information which [they] transmit or store' or 'actively to seek [new] facts or circumstances indicating illegal activity'. This typically applies to orders asking for the 'stay-down' of information, 'prevention of re-appearance', or those requiring 'dynamic updating'.[13]

The liability chapter of the DSA is based on the idea that facts are gathered and evaluated usually by victims, and hosting providers only check their requests for manifest illegality.[14] When orders or statutory obligations ask providers to continue to acquire

[9] Crabit (n 5) 815.

[10] Arguably, this also means that imposing direct liability for illegal content hosted on its service usually represents a breach of the liability exemption and the general obligation to monitor.

[11] This seems to be suggested by the AG in Case C-314/12 *UPC Telekabel Wien GmbH v Constantin Film Verleih GmbH* ECLI:EU:C:2013:781, Opinion of AG Cruz Villalón, para 78.

[12] Martin Husovec, 'Holey Cap! CJEU Drills (yet) Another Hole in the e-Commerce Directive's Safe Harbours' (2017) 12(2) Journal of Intellectual Property Law & Practice 115, 119.

[13] For the practice in the Member States, see EUIPO and CEIPI, *Study on Dynamic Blocking Injunctions in the European Union* (EUIPO 2021) <https://op.europa.eu/s/yX4r> accessed 21 August 2023.

[14] See ch 7.

new information, they modify liability exemptions because first, they oblige providers to know, and then punish them for knowing. The problem does not arise, however, if the measure is prospective, but the new information continues to be supplied by victims. This is the case for dynamically updated website blocking injunctions that change their target after they are granted by judges.[15] The key consideration in such cases is the question of oversight.

The DSA does not make all monitoring or fact-finding obligations illegal. However, it allows them only if they are specific, ie if they are properly targeted. One can clearly draw an analogy with data retention. Article 8 DSA prevents indiscriminate surveillance of digital content and people using the internet but permits the legitimate targeted actions of authorities.[16] Surveillance measures imposed on providers to fight illegal content or behaviour online are not entirely prohibited, but they must be administrated by authorities, be proportionate and strictly targeted—at least unless the EU legislature says otherwise. Thus, a court order asking providers to preserve or release evidence, or observe a specific user, easily satisfy the requirements of Article 8 DSA. However, once the orders extend to the broader digital public, the difficulties start.

5.2.3 When is it 'general'?

Based on Recital 47 ECD, pre-DSA case law quickly distinguished specific and general monitoring. While specific monitoring is permitted, general monitoring is prohibited by Article 15 ECD. Where the boundary lies exactly, however, has become a longstanding contention between the CJEU and Member States, and even within the CJEU. Over the years, the EU legislature adopted legislation that reiterates the GMOP in very different sectorial legal instruments to complicate things further. It is, therefore, possible that the GMOP carries different meanings in different contexts.

Early case law interpreted general monitoring as measures that concern large parts of the user base of a particular service. Thus, searching content posted by everyone would be seen as general, even if it was performed to find something particular (eg an image depicting the abuse of a particular child). Thus, knowing what needle you are looking for does not justify searching the entire haystack. The interpretation was devised first by the Grand Chamber of the CJEU in *L'Oréal v eBay* in 2011,[17] and it was then applied by a five-judge chamber in the *SABAM* and *Scarlet Extended* cases in 2012.[18]

[15] See, for instance, the decision of the District Court of Hague, Rb Den Haag 22 September 2017, Case C/09/535341, ECLI:NL:RBDHA:2017:10789 (*Stichting Brein/Ziggo & XS4ALL*), para 5.3 ('orders [an ISP] in the event that TPB starts operating via other/additional IP addresses and/or (sub)domain names … to block and keep blocked the access of their customers to these … within three working days after delivery by Brein').

[16] A similar opinion is presented by Folkert Wilman, 'Two Emerging Principles of EU Internet Law: A Comparative Analysis of the Prohibitions of General Data Retention and General Monitoring Obligations' (2022) 46 CLS Review 105728.

[17] *eBay* (n 7) para 139.

[18] *SABAM* (n 7); *Scarlet Extended* (n 7).

In *eBay*, the CJEU ruled that an injunction imposed on an online marketplace, as a type of measure, 'cannot have as its object or effect a general and permanent prohibition on the selling, on that marketplace, of goods bearing those trademarks'.[19] The Court applied the standard proposed by AG Jääskinen,[20] and it accepted that measures consisting of a suspension of accounts or measures enabling identification of its sellers would be sufficiently specific.[21] The Court noted that the two mentioned measures are not the only ones possible.[22] The German courts took this to mean that the applied standard is not exhaustive,[23] which was arguably wrong because the CJEU clearly referenced[24] the following standard properly articulated by AG Jääskinen:

> An appropriate limit for the scope of injunctions may be that of a double requirement of identity. This means that the infringing third party should be the same and that the trade mark infringed should be the same in the cases concerned. Hence, an injunction could be given against an intermediary to prevent the continuation or repetition of an infringement of a certain trade mark by a certain user. Such an injunction could be followed by an information society service provider by simply closing the client account of the user in question.[25]

In *Sabam* and *Scarlet Extended*, a national court considered whether an internet access provider and a social networking platform could be asked to install filtering systems. The CJEU concluded that this would involve the 'systematic analysis of all content and the collection and identification of users' IP addresses from which unlawful content on the network is sent'.[26] This was viewed as too general. On the other hand, in *UPC Telekabel*, the CJEU accepted website blocking measures as a legitimate and specific type of monitoring when it followed the advice given by the AG:

> It would constitute such an inadmissible measure if the court had ordered the ISP actively to seek copies of the infringing page among other domain names or to filter all the data carried in its network in order to ascertain whether they constitute transfers of specific protected film works and to block such transfers. However, such a measure is not in issue in the present case. Rather, the referring court is required to decide on the blocking of a specific website. The measure therefore does not infringe Article 15(1) of Directive 2000/31.[27]

[19] *eBay* (n 7) para 140.
[20] Case C-324/09 *L'Oréal SA and Others v eBay International AG and Others* ECLI:EU:C:2010:757, Opinion of AG Jääskinen, para 182.
[21] *eBay* (n 7) paras 141–42.
[22] ibid paras 141–43.
[23] See German Federal Supreme Court cases, BGH v 22 July 2010 – I ZR 139/08 *(Kinderhochstuehle im Internet I)*; BGH v 12.07.2012 – I ZR 18/11 (*Alone in the dark*); BGH v 15 August 2013 – I ZR 80/12 *(File-Hosting-Dienst)*; BGH v 16 May 2013 – I ZR 216/11 *(Kinderhochstühle im Internet II)*.
[24] *eBay* (n 7) para 141, pointing to the part with standard.
[25] *eBay* (Opinion of AG Jääskinen) (n 20) para 182.
[26] *Scarlet Extended* (n 7) para 40; *SABAM* (n 7) para 38.
[27] *UPC Telekabel (Opinion of AG Cruz Villalón)* (n 11) para 78, suggests this.

This reasoning was not without problems, in particular, because website blocking is an enforcement goal that can be implemented in a number of ways. Some blocking can take the form of specific monitoring (as defined by *eBay*), such as when a Domain Name System (DNS) entry is blocked. However, Deep Packet Inspection (DPI) based blocking, which scans all data carried in the network as it passes an inspection point, constitutes indiscriminate monitoring. The CJEU did not consider this point and simply approved website blocking as an enforcement goal.

In the *McFadden* case, concerning a wi-fi hotspot, AG Szpunar argued that 'a measure requiring the owner of an internet connection to examine all communications transmitted through that connection' would 'clearly conflict with the prohibition on imposing a general monitoring obligation'.[28] In his view, 'in order to constitute a monitoring obligation "in a specific case", such as is permitted under Article 15(1), the measure in question must be limited in terms of the *subject* and *duration* of the monitoring, and that would not be the case with a measure that entailed the examination of all communications passing through a network'.[29] Thus, Szpunar proposed to use the subject and duration as the limiting principles. The Court accepted the conclusion of the AG's analysis and ruled that 'examining all communications passing through an internet connection' is a violation of the GMOP without explicitly referring to the two conditions.[30] It should be recalled that the Court already spoke of 'general and *permanent*' obligations as being incompatible in *eBay*. Therefore, AG Szpunar's view had a firm footing in the case law.

In *Tommy Hilfiger*, a case dealing with the obligation in the offline context (preventive obligations imposed on a flea market operator), the Court restated its case law, weaving in also requirements of the IP Enforcement Directive, as follows:

> Lastly, the Court held that injunctions must be equitable and proportionate. They must not therefore be excessively expensive and must not create barriers to legitimate trade. Nor can the intermediary be required to exercise general and permanent oversight over its customers. By contrast, the intermediary may be forced to take measures which contribute to avoiding new infringements of the same nature by the same market-trader from taking place.[31]

The 'general and *permanent* oversight of customers' is equivalent to 'general and permanent monitoring' known from *eBay*. Similarly, in line with that ruling, the decision seemed to again suggest that the only specific oversight that would be acceptable is one limited to 'avoiding new infringements of the same nature by the same market trader from taking place'.

[28] Case C-484/14 *Tobias McFadden v Sony Music Entertainment Germany GmbH* ECLI:EU:C:2016:170, Opinion of AG Szpunar, para 132.
[29] ibid.
[30] *McFadden* (n 8) para 87.
[31] Case C-494/15 *Tommy Hilfiger Licensing LLC and Others v Delta Center* ECLI:EU:C:2016:528, para 34.

This case law was largely consistent, although not universally followed, until 2019, when the CJEU decided the *Glawischnig* case.[32] Before I explain that ruling, it is crucial to understand the precedential weight of all these decisions. The only Grand Chamber ruling from the cases above is *eBay*. All other rulings, including *Glawischnig*, are 'only' five-judge rulings. In *SABAM* and *Scarlet Extended*, the judge rapporteur was one of the leading copyright judges, Malenovský.[33] In the only Grand Chamber judgment, *eBay*, the rapporteur was another leading IP judge, Ilešič. The *Glawischnig* ruling was authored by Malenovský just before he retired from the bench.[34]

In *Glawischnig*, the CJEU accepted that specific monitoring could also entail automated tools applied to the entire user base to locate and block a specific infringement. If the needle sought was specifically identified (eg a website or a specific piece of content), the haystack could span the entire service. The Court argued that if the *instructions* for the continuous search were specific enough, the analysis of all content on the service would not be against the GMOP. The important caveat was that the case, unlike all earlier IP cases, concerned defamation, and the national measure subject to scrutiny was a judgment spelling out such instructions and identifying which exact expressions were illegal. Thus, the obligations resulted from a judge applying the law to specific facts and instructing the platform on what exact content must be removed and prevented. This was a clear shift from the Court's previous position. AG Szpunar's opinion was willing to impose future filtering of content only upon the same user—thus searching only in a related haystack.[35]

The five-judge chamber explained its new position as follows:

> (41) It follows therefore that, in order for an injunction which is intended to bring an end to an illegal act and to prevent it being repeated, in addition to any further impairment of the interests involved, to be capable of achieving those objectives effectively, that injunction must be able to extend to information, the content of which, whilst essentially conveying the same message, is worded slightly differently, because of the words used or their combination, compared with the information whose content was declared to be illegal. Otherwise, as the referring court made clear, the effects of such an injunction could easily be circumvented by the storing of messages which are scarcely different from those which were previously declared to be illegal, which could result in the person concerned having to initiate multiple proceedings in order to bring an end to the conduct of which he is a victim …

[32] *Glawischnig* (n 7).

[33] For the analysis of how the judges start de facto specialising, see Eleonora Rosati, *Copyright and the Court of Justice of the European Union* (2nd edn, OUP 2023).

[34] The Court held that a website blocking measure does not have to specify the means as long it targets a specific website. However, this could also mean that the measure is only specific under the old understanding (eg domain name blacklisting) but also includes measures that scan the entire contents of transmitted communications (eg DPI technology to spot the targeted website). This aspect was later criticised by other members of the Court, such as the AG, see *McFadden* (Opinion of AG Szpunar) (n 28).

[35] *Glawischnig (Opinion of AG Szpunar)* (n 3) para 75.

> (45) In light of the foregoing, it is important that the equivalent information referred to in paragraph 41 above contains specific elements which are properly identified in the injunction, such as the name of the person concerned by the infringement determined previously, the circumstances in which that infringement was determined and equivalent content to that which was declared to be illegal. Differences in the wording of that equivalent content, compared with the content which was declared to be illegal, must not, in any event, be such as to require the host provider concerned to carry out an independent assessment of that content.
> (46) In those circumstances, an obligation such as the one described in paragraphs 41 and 45 above, on the one hand—in so far as it also extends to information with equivalent content—appears to be sufficiently effective for ensuring that the person targeted by the defamatory statements is protected. On the other hand, that protection is not provided by means of an excessive obligation being imposed on the host provider, in so far as the monitoring of and search for information which it requires are limited to information containing the elements specified in the injunction, and its defamatory content of an equivalent nature does not require the host provider to carry out an independent assessment, since the latter has recourse to automated search tools and technologies.[36]

The decision was immediately understood as a departure by other AGs[37] and academic commentators.[38] According to Angelopoulos and Senftleben,[39] however, its reach should remain confined to defamation and be understood as chipping away from the baseline *eBay* standard only when judges issue specific instructions. Thus, even the new lowered standard, in their view,[40] does not permit national legislatures to use measures that would operate without judicial authorisation in each case.

The major difficulty with *Glawischnig* is that it does not consider the limits of the potentially continuous order. In the analogous online world, few judges would issue permanent search warrants without oversight. A warrant targeting a company that orchestrates public and private communications would be unthinkable without due consideration given to time and tailoring of the order's scope to avoid overreaching. The Court in *Glawischnig* refused to engage on all these points because it remains silent on what additional safeguards, if any, are required to grant the order.

A few months after *Glawischnig*, the CJEU issued a Grand Chamber decision on a related issue. In *Poland v Council/EP*, the Court reinforced the logic behind the *Glawischnig* ruling.[41] Here, the Court scrutinised an EU legislation that 'required to

[36] *Glawischnig* (n 7) paras 41, 45, and 46 (emphasis mine).
[37] Case C-401/19 *Republic of Poland v European Parliament and Council of the European Union* ECLI:EU:C:2021:613, Opinion of AG Øe, paras 112–13; Daphne Keller, 'Facebook Filters, Fundamental Rights, and the CJEU's Glawischnig-Piesczek Ruling' (2020) 69(6) Journal of European and International IP Law 616.
[38] Christina Angelopoulos and Martin Senftleben, 'An Endless Odyssey? Content Moderation Without General Content Monitoring Obligations' (2021) <https://ssrn.com/abstract=3871916> accessed 1 August 2023.
[39] ibid 18, 22.
[40] ibid 4.
[41] *Poland* (n 8).

use automatic recognition and filtering tools'[42] at the mere request of right holders. According to the Court, although the GMOP was mentioned in the legislation, it was not violated but rather acted as a safeguard. The Court explained it as follows:

> Fourthly, by stating, in terms similar to those employed in Article 15(1) of Directive 2000/31 in respect of that directive, that the application of Article 17 of Directive 2019/790 must not lead to any general monitoring obligation, Article 17(8) of that directive provides an *additional safeguard for ensuring that the right to freedom of expression and information of users of online content-sharing services is observed* …[43]

Thus, the Court accepted that the entire user base of a video-sharing service can be subject to monitoring and that the specific instructions do not have to be issued by a court. On the one hand, the Court confirms that the GMOP is not violated if the specific instructions come from individuals without pre-existing judicial determination. On the other, unlike judicial injunctions, the legal basis was an act of Union law that also included additional safeguards, where a restatement of the GMOP only served as one of such safeguards. In other words, while the principle of general monitoring was invoked by the state, the legislation was not that of the Member State but the Union, and it was accompanied by additional safeguards. In my view, for the Court, this spoke in favour of loosening up the GMOP standard since there was no concern that the Member States would fragment the single market or that the national authorities do not provide some level of supervision.

The main focus of CJEU's judgment in *Poland* is on strict targeting of measures and the level of errors. The Court notes that filtering and blocking upon upload constitutes a prior restraint and thus cannot lead to the blocking of legal content. The technology can be used but must 'distinguish adequately between unlawful content and lawful content'.[44] This seems non-negotiable for the Court. The Court in *Poland* notes that the technology put in place must also comply with 'an additional safeguard'.[45] It must achieve such adequacy without 'an independent assessment of the content' of facts or law. In my view, this means that machines must be capable of satisfying the standard without human involvement. Here is how the Court expresses it:

> 90 … That clarification means that the providers of those services *cannot be required to prevent the uploading and making available to the public of content which*, in order to be found unlawful, *would require an independent assessment of the content* by them in the light of the information provided by the rightholders and of any exceptions and limitations to copyright (see, by analogy, judgment of 3 October 2019, *Glawischnig-Piesczek*, C-18/18, EU:C:2019:821, paragraphs 41 to 46).[46]

[42] ibid para 54.
[43] ibid para 90 (emphasis mine).
[44] ibid 86; *Scarlet Extended* (n 7) para 52; *SABAM* (n 7) para 50.
[45] *Poland* (n 8) para 90.
[46] ibid (emphasis mine).

And this is the referenced text from *Glawischnig*:

> 46 In those circumstances, an obligation … appears to be sufficiently effective for ensuring that the person targeted by the defamatory statements is protected. On the other hand, that protection is not provided by means of an excessive obligation being imposed on the host provider, in so far as the monitoring of and search for information which it requires are limited to information containing the elements specified in the injunction, and its defamatory content of an equivalent nature *does not require the host provider to carry out an independent assessment, since the latter has recourse to automated search tools and technologies.*[47]

In my view, this means that the limit of the GMOP is what the technology in question can do *autonomously*.[48] The Court understands independent assessment as an assessment of facts or law which requires recourse to non-automated tools, which can only mean human judgement. The reason is linguistic but also teleological. If the same need for assessment is triggered by a notification, it would clearly be labelled as an independent assessment. Moreover, *if* an upfront obligation to review uploaded content by humans is illegal, it should not make any difference *how* the sample for manual review is generated. Thus, if it is illegal to mandate humans to do sample checks a priori, the same should be true if such sample checks are mandated to sort out errors generated by machines.

Only the machine-only configuration does not increase the stock of knowledge. Whatever a machine sees does not lead to actual knowledge of the provider and thus cannot lead to liability. The opposite reading, ie that faulty technology can generate many false positives that humans must review even only for obvious errors, would mean that those generated false positives might lead to actual knowledge and thereby strip providers of liability exemptions exactly because they are reviewed by humans—the very point that the GMOP tries to prevent.

Even in the context of Article 17 of the Copyright in the Digital Single Market (CDSM) Directive, the technology used must be precise enough. While the Court does not go into the details, this also has consequences for what can be subject to such user-base-wide orders. If infringements cannot be identified and evaluated with a negligible margin of error, there can be no expectation that machines can meaningfully help in uncovering them. This is why I think that the Court is permitting user-base-wide measures only for 'automatable infringements'.[49]

[47] *Glawischnig* (n 7) paras 45–46 (emphasis mine).

[48] Martin Husovec, 'Mandatory Filtering Does Not Always Violate Freedom of Expression: Important Lessons from *Poland v Council and European Parliament*' (2023) 60(1) Common Market Law Review 173.

[49] I have previously developed this concept to explain when infringements can be spotted by technology with a negligible margin of error: Martin Husovec, 'The Promises of Algorithmic Copyright Enforcement' (2018) 42(1) Columbia Journal of Law & the Arts 53.

Thus, if humans must get involved to complement automation to assure the adequacy of error rates, their involvement rightly triggers the GMOP. While this reading is intuitive, it is not followed by some Member State courts.[50]

So—where does this leave us?

It is indisputable that the CJEU gradually broadened its standard for what constitutes permissible monitoring under Article 15 ECD. In my view, the Court is currently moving away from user-specific tailoring to a more flexible test. Arguably, three main factors determine whether monitoring is general and prohibited, or specific and allowed: (a) specificity of instructions, (b) adequate automatability of implementation, and (c) existence of safeguards. The maximisation of these factors leads to strict targeting for speech, privacy and data protection concerns, and proportionality for the right to conduct business.

Specificity of instructions requires that a legal mandate (an order or law) must specify whose rights are protected, which exact rights, and which infringements must be prevented. The type of violation subject to the request must be sufficiently narrow. For instance, the request cannot concern just any violation of personality rights but must be limited to the same or almost identical expressions of already identified offensive comments. While the Court does not require one specific technological implementation, it seems to insist that at least the enforcement goals, such as blocking of a website, removal, and reappearance, are formulated with sufficient precision. This means a request asking 'any infringement' to 'disappear' from the service would fail.

Whenever specific instructions try to prevent some acts of users, their implementation must be susceptible to adequate automation. It cannot go beyond what machines can implement with adequate precision.[51] In my view, if there is no way for a provider to automate compliance, no proactive action is required to satisfy preventive duties. Providers might bear the burden of proof to justify this, but if proven, the inability to adequately automate should exonerate them from the obligation. If this were not the case, the providers would be forced to employ humans to seek and assess facts, which would violate the GMOP.[52] Thus, for instance, demanding that platforms use filters that are so imprecise that they must be complemented by humans should violate the GMOP, as would requiring them to check individual pieces of content before such filters are put into place.

The specificity of instructions and their scalability through automation achieves a fair balance because it reduces the effort and resources the providers must put in place. In the spirit of Article 7 DSA, it insulates desirable behaviour—compliance with injunctions—from being a potential source of new liability risks for the provider—knowledge of new violations—to avoid disincentivising it. Because the burden for

[50] See the German Federal Supreme Court case before the *Glawischnig* ruling, *Alone in the Dark* (n 23). and the Austrian Supreme Court case after the *Glawischnig* ruling, also allowing expansion to laypersons, OGH 30 March 2020, 4 Ob 36/20b SZ 2020/25, para 6.1.

[51] While this is not entirely clear from *Poland* (n 8) para 90, it is clear from *Glawischnig* (n 7) para 46.

[52] This does not preclude providers from relying on humans in the process, but their involvement cannot be used as an excuse for lowering the standard.

social harms online is shared (see Chapter 21), each party is required to do their part, and providers cannot be asked to conduct 'a detailed legal examination'[53] or seek out new facts as it would represent 'a burden in excess of what can reasonably be expected'.[54]

The existence of the appropriate legal mandate supervised by authorities is also crucial for the observance of safeguards—an implicit third requirement in case law. In fact, the presence of authorities that oversee the grant is already one such safeguard. The other can take different forms, such as advanced notice to affected parties, their ability to challenge orders or their implementation, time limits for orders, or disclosures and transparency. The CJEU has so far addressed these points in its discussion of proportionality;[55] however, they are clearly inextricably connected with the legal basis.

Once the instructions are specific, they must still pass the requirement of being prescribed by the law and proportionate, including being subject to sufficient safeguards. In the absence of Union legislation to the contrary, the instructions to trigger monitoring must always be issued by the authorities. This is not because of Article 8 DSA but due to the interpretation of liability exemptions (see Chapter 6). Obligations to perform specific monitoring, subject to penalties of any kind, are a form of liability for information. They are thus caught by liability exemptions but are, in turn, released by injunction clauses to preserve 'the possibility for a court or administrative authority' to issue orders. In other words, even specific monitoring obligations compatible with the GMOP can still only be issued by authorities. As a result, specific monitoring cannot be triggered by a request of a private party merely enabled by legislation. Only if an authority is involved in conferring such obligation does the liability exemption not stand in the way. National law giving power to individuals to legally request specific monitoring without any involvement of authorities violates the DSA.[56]

Thus, even under the most favourable interpretation of Article 8 DSA, national non-judicial or non-administrative stay-down obligations (obligations to prevent future recurrence of infringement) are not compatible with Articles 4–6 DSA unless the EU legislature introduced them. For all other cases, only national decisions issued by authorities, if they include specific instructions, can lead to such obligations. The non-judicial or non-administrative stay-down can only be introduced in some form by the EU legislature, as we have seen in the case of Article 17 CDSM Directive.

The CJEU still seems to be in the process of outlining what exactly constitutes an illegal general monitoring obligation.[57] A lot more case law can be expected on the matter in the coming years. However, given that the DSA is a measure of full harmonisation providing for a complex system of mechanisms to tackle illegal content online,

[53] Joined Cases C-682/18 and C-683/18 *Frank Peterson v Google LLC and Others and Elsevier Inc v Cyando AG* ECLI:EU:C:2021:503, para 116.

[54] Case C-460/20 *TU and RE v Google LLC* ECLI:EU:C:2022:962, para 71.

[55] *UPC Telekabel* (n 8) para 57.

[56] To be sure, laws allowing merely request-based specific monitoring can be legislated but are reserved for the EU legislature. The EU legislature can naturally amend the DSA itself. We have witnessed this in *Poland*—a case reviewing the constitutionality of art 17 CDSM Directive.

[57] Andreas Paulus, 'Schutz des geistigen Eigentums' in Josef Isensee and Paul Kirchhof (eds), *Handbuch des Staatsrechts der Bundesrepublik Deutschland* (Band XI, C. H. Beck 2013) § 247, paras 49–51.

it is difficult to find space for national laws imposing other proactive obligations in their legislation anyway (see Chapter 17).[58] The GMOP will thus serve as an important European backstop against indiscriminate surveillance of people and content.

5.3 Origins of the GMOP: From the ECD to the DSA

Having attempted to demarcate the scope of the GMOP, it is useful to examine its legislative history and developments up to this point. Article 8 DSA essentially serves as a 'bridge of continuity'[59] for the GMOP between the ECD and the DSA. However, the provision is slightly reworded to better fit into a regulation. Table 5.1 illustrates the changes.

First, given the change from a directive to a regulation, the prohibition is no longer directed to the Member States ('Member States shall not'). Instead, a passive form is used to express a general prohibition ('no … shall be imposed'). Article 8 DSA thus clearly formulates a substantive principle rather than merely a procedural rule limiting state action. This brings about no change for state actions on the national level, such as orders issued by authorities or legislative acts. It might, however, change or clarify how Article 8 DSA covers state action of EU bodies (eg by the European Commission) and whether it also covers non-state actors. Article 15 ECD did not explicitly cover EU bodies as it only spoke of the Member States. Article 8 DSA widens the scope by turning the language from specific to all-encompassing. Given the powers that the European Commission gains with the DSA, it is only natural that the GMOP also explicitly started applying to the EU bodies.

Second, while the ECD included a cross-reference to a provider 'when providing the services covered by Articles 12, 13 and 14' (ie those with the liability exemptions), the

Table 5.1 GMOP in the ECD and DSA

GMOP in Article 15 ECD	GMOP in Article 8 DSA
'*Member States shall not* impose a general obligation on providers, when *providing the services covered by Articles 12, 13 and 14*, to monitor the information which they transmit or store, nor a general obligation actively to seek facts or circumstances indicating illegal activity'.	'No general obligation to monitor the information which *providers of intermediary services* transmit or store, nor actively to seek facts or circumstances indicating illegal activity *shall be imposed* on those providers'.

[58] If the measure at stake undermines the DSA mechanisms, it can be pre-empted by such DSA provisions without even invoking the GMOP. For instance, art 22 DSA would pre-empt national authorities from issuing injunctions obliging providers to prioritise assessment of notifications even from entities that do not qualify as trusted flaggers; art 23 would pre-empt injunctions requiring that no prior warning be served prior to account blocking.

[59] *Interview with Irene Roche Laguna*, Deputy Head of Unit for Coordination and Regulatory Compliance, European Commission (2021–23). The interview was carried out over a number of sessions across the three years.

Table 5.2 Recital 47 ECD vs. Recital 30 DSA

Recital 47 ECD	Recital 30 DSA
'Member States are prevented from imposing a monitoring obligation on service providers only with respect to obligations of a general nature; this does not concern monitoring obligations in a specific case and, in particular, does not affect orders by national authorities in accordance with national legislation'.	'Providers of intermediary services should not be, neither de jure, nor de facto, subject to a monitoring obligation with respect to obligations of a general nature. This does not concern monitoring obligations in a specific case and, in particular, does not affect orders by national authorities in accordance with national legislation, in compliance with Union law, as interpreted by the CJEU, and in accordance with the conditions established in this Regulation. Nothing in this Regulation should be construed as an imposition of a general monitoring obligation or a general, active fact-finding obligation, or as a general obligation for providers to take proactive measures to in relation to illegal content'.

DSA refers merely to 'intermediary services' along with the technical activities of transmitting or storing. This could be read as a mere simplification of the text, but it could also be read as stipulating that the prohibition of general monitoring *does* apply *whenever* providers exercise those technical functions, *regardless* of whether they eventually lose a liability exemption because they stop being neutral (see Chapter 6).

Finally, the last cosmetic change is that the second paragraph of Article 15 ECD is dropped entirely. It made sense in a minimum harmonisation instrument like the ECD but not in a full harmonisation instrument. The DSA covers some ways under which the Member States' actors can obtain information from digital intermediaries regarding the identity of their users. In fact, in the context of the discussions leading to the adoption of the ECD, it was thought that this paragraph was unnecessary from a legal perspective since no provision of the Directive had the potential effect of limiting the possibility of legislation by the Member States.[60] Article 15(2) ECD was only added to ensure that such national laws could not derogate from the liability exemptions.[61] A similar cosmetic change is the title of the article which shifts from '[n]o general obligation to monitor' to '[n]o general monitoring or active fact-finding obligations'.

There has also been a change in the accompanying Recitals. Under the ECD, the most important arguments were found in Recital 47. In DSA, it is Recital 30. The table below shows how they compare. The EU co-legislators wanted to add a 'dynamic reference' to the rich case law established by the CJEU. The text clearly states that the DSA must be subjected to the same case law of the CJEU as under the ECD. The co-legislators agreed upon this dynamic reference at the last minute after a long debate regarding a slightly erratic attempt at 'codifying' some elements of such case law, as proposed by the Council (see Table 5.2).

[60] ibid.
[61] Crabit (n 5) 816.

Firstly, Recital 30 DSA stipulates that specific monitoring obligations, in particular those imposed by national orders, should be issued in compliance with Union law, including the EU Charter. Already under the ECD, these orders were within the remit of EU law because orders permitted by injunction clauses were technically derogations that had to comply with the GMOP.[62] This clarification, along with provisions like Article 9 DSA on orders, renders the conclusion inescapable.

Secondly, Recital 30 DSA emphasises that provisions of the DSA itself are equally subject to the GMOP. This is a crucial reminder, given that the DSA has numerous tools that could be interpreted broadly. For instance, the risk-based measures applicable to VLOPs and very large online search engines (VLOSEs), or the 'best efforts' obligations imposed on online marketplaces, when interpreted in light of Article 8 DSA, may not de facto or de jure lead to an obligation to generally monitor or fact-find illegal content, including the 'general obligation [to take] proactive measures'.[63] These obligations are legislated next to liability exemptions as special rules that indirectly amend liability exemptions, but under the condition that they remain targeted as required by the GMOP.[64]

5.4 The GMOP as a Balancing Tool

The prohibition of general monitoring is a reflective surface for many freedom of expression, privacy and data protection concerns in the digital environment. It de facto constitutes a tool for constitutional balancing. Looking at its wording, one would easily think that the most important right that the GMOP protects is the right to conduct business (Article 16 EU Charter of the Fundamental Rights (CFR)).[65] However, as was mentioned in the introduction, the most frequently protected right that the GMOP guarantees is actually the right to freedom of expression and information (Article 11 CFR). So far, it is less understood that the GMOP equally protects personal data and privacy (Articles 7–8 CFR). Table 5.3 lists examples of typical measures and risks in the context of Article 8 DSA.

To date, the typically mentioned policy rationale of the GMOP has been that it protects against blocking lawful content due to limits of technology. Arguably, Recital 26 now reinforces this focus by stating that 'providers … should, for example, take reasonable measures to ensure that, where automated tools are used to conduct such activities, the relevant technology is sufficiently reliable to limit to the maximum extent possible the rate of errors'. In this sense, Article 8 DSA acts as a brake on using technological

[62] On the injunction clauses (arts 14(3), 13(2), and 12(3) ECD), ch 8.
[63] DSA, Rec 30.
[64] In the absence of European harmonisation, enforcing some of the due diligence rules, such as fines for failing to engage in risk mitigation, would fall under the remit of the liability exemptions and be barred by them in the national law. The EU thus opened the regulatory space; however, it only used the tools in the DSA.
[65] Charter of Fundamental Rights of the European Union [2012] OJ C326/391, art 16.

Table 5.3 Keys risks for general monitoring

	Freedom of expression	**Privacy and data protection**	**Right to conduct business**
High risks	Over-blocking of legal information caused by inadequate automation	Preventive indiscriminate surveillance of people's private communications	Preventive obligations that require independent fact-gathering or assessment
Low risks	Reactive measures to remove specific content or block specific users	User-targeted measures	Reactive measures to remove specific content or block specific users

solutions that might be inadequate from the perspective of freedom of expression. As explained by the CJEU:

> … A filtering system which might not distinguish adequately between unlawful content and lawful content, with the result that its introduction could lead to the blocking of lawful communications, would be incompatible with the right to freedom of expression and information, guaranteed in Article 11 of the Charter, and would not respect the fair balance between that right and the right to intellectual property. … The providers of those services cannot be required to prevent the uploading and making available to the public of content which, in order to be found unlawful, would require an independent assessment of the content by them in the light of the information provided … [66]

This reading was suggested by AG Øe, who felt that given the technological improvements, the CJEU had already approved more permissive standards of the GMOP in *Glaswischnig*.[67] The most compelling description of the GMOP's function can be found in the following passage, where he summarised it as follows:

> I am inclined to regard the prohibition laid down in Article 15 of Directive 2000/31 as a general principle of law governing the Internet, in that it gives practical effect, in the digital environment, to the fundamental freedom of communication. I note, moreover, that the Court has already brought together compliance with that freedom and that prohibition in its case-law. One cannot exist without the other. It follows, in my view, that that prohibition goes beyond the scope of Article 15 of Directive 2000/31 and is binding not only on the Member States, but also on the EU legislature.[68]

The AG rightly evoked the case law of the CJEU, which previously dressed up its rejection of the national measures in the EU Charter's cloth.[69] The CJEU eventually fully

[66] *Poland* (n 8) paras 86, 90.
[67] *Poland (Opinion of AG Øe)* (n 37) para 113.
[68] ibid para 106.
[69] *Scarlet Extended* (n 7) paras 40, 52; *SABAM* (n 7) paras 38, 50.

accepted this reading by AG Øe when it ruled that the GMOP constitutes 'an additional safeguard for ensuring that the right to freedom of expression and information of users of online content-sharing services is observed'.[70] As discussed above, in having the speech concerns of content creators in mind, this had led to several important limiting principles: (a) strict targeting of measures, (b) adequacy of error rates, and (c) machine-only implementation of the tools. While these measures protect providers against excessive demands, the right to conduct business, in fact, shapes the measures less than the right to freedom of expression and information. For instance, the adequacy of error rates actually raises costs for providers who could employ cheaper solutions. The Court's failure to constantly articulate this[71] should not be immediately seen as a failure to recognise this trade-off.

Thus, the GMOP emphasises the precision of enforcement rather than its cost to providers. If delivering adequate quality is more expensive but still proportionate, the GMOP arguably demands that quality be given preference. This never-ending compromise between cost and precision is also evident in the requirement for preventive measures, whereby machines must, in themselves, be able to deliver such adequate quality. In the end, this protects providers from excessive demands to employ human moderators to complement faulty technologies, but it protects speakers exposed to faulty decision-making. Taken together, the GMOP acts as an incentive to improve technological means.

The above argument was brought to a close by the European Commission, who much earlier speculated that: 'one can imagine that if filtering techniques had become flawless and costless, the need for a prohibition on imposing a general monitoring obligation would have become obsolete'.[72] But is it true? If automated tools were to become flawless, would this render the GMOP superfluous?

First, it is fairly clear that such a flawless state can never be reached. No technology can avoid making mistakes, more so if applied to contextually sensitive legal assessments. No amount of machine learning and great data sets will change that. More realistically, automated tools may become sufficiently good in some areas so that they can outperform humans in the rate of their errors.[73] This would constitute a tremendous improvement. Of course, such tools could hardly ever become costless as they would require access to new data sets. Plus, the laws determining their assessments change as well. The most realistic expectation is that technological tools will become better than humans at some point and thus can be deployed in many more areas than today and at lower costs. This will obviously broaden their deployment.

[70] *Poland* (n 8) paras 86, 90.

[71] Most obviously in *Glawischnig* (n 7). As argued in ch 3, the Court is often influenced by the framing in its responses, which does not immediately mean that what goes unmentioned is entirely left out of the picture.

[72] Commission, '"Online Services, Including e-Commerce, in the Single Market" (Commission Staff Working Document) Accompanying the Document "A Coherent Framework to Boost Confidence in the Digital Single Market of e-Commerce and Other Online Services"' (Communication) SEC(2011) 1641 final, 50.

[73] Husovec, 'The Promises of Algorithmic Copyright Enforcement' (n 49) 67–69.

However, even perfect tools can still implicate data protection rights and constitutional issues around mass surveillance. One might still worry about the impressive efficiencies of imaginary error-free systems. Such systems could be viewed as autonomously seeing and deciding too much. The automated tools can draw on years of data and assess many aspects of people's lives. They could provide efficiencies that inevitably come at the expense of the privacy and agency of individuals. Thus, it is hard to imagine that even error-free tools would ever make the GMOP entirely redundant. Better technology will only highlight the data protection dimension. At the moment, the freedom of expression dimension seems justifiably more central. As technologies progress, this may change.[74]

It seems less known that the CJEU previously conceptualised the GMOP in light of both Articles 8 and 11 of the EU Charter, thus also covering the right to personal data among its functions.[75] Automated tools of enforcement, such as filters, sometimes need personal data (eg videos depicting persons). The long-term retention of such data, its processing in reference databases, often through profiling, and the ability to reach automated decisions are all obvious concerns of data protection law. Privacy concerns have been less important in much of today's case law dealing with IP rights because content recognition technologies sometimes avoid processing personal data. However, in other areas, such as face or voice recognition, personal data will have to be used. This is already the case with filtering technologies such as PhotoDNA, which processes highly sensitive photographs of child abuse material.

There is no doubt that many measures that could qualify as general monitoring, even in the absence of Article 8 DSA, would need to be scrutinised under other EU acts in the data protection law[76] and the CJEU case law on data retention and automated assessment.[77] During the legislative process, the European Parliament suggested including explicit safeguards against various cases of abuse of personal data in Article 8 DSA. However, that proposal was not adopted.

To conclude, the GMOP, at its core, protects individuals against indiscriminate surveillance of their behaviour and expressions.[78] It also protects providers from

[74] This was precisely the argument raised by the European Parliament when proposing modifications to art 8 that would prohibit the imposition of automated tools for content moderation, the provision of end-to-end encrypted services or the anonymous use of the services. European Parliament, 'Amendments adopted by the European Parliament on 20 January 2022 on the proposal for a regulation of the European Parliament and of the Council on a Single Market For Digital Services (DSA) and amending Directive 2000/31/EC ((COM(2020)0825 — C9-0418/2020 — 2020/0361(COD)))' [2022] OJ C336/48, 138.

[75] *Scarlet Extended* (n 7) para 50: '… as the contested filtering system may also infringe the fundamental rights of that ISP's customers, namely their right to protection of their personal data and their freedom to receive or impart information, which are rights safeguarded by Articles 8 and 11 of the Charter respectively'. However, the Court did not invoke art 15 ECD specifically in this context.

[76] Council Regulation (EC) 2016/679 of 27 April 2016 on the protection of natural persons concerning the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC [2016] OJ L119/1 (GDPR); European Parliament and Council Directive (EU) 2016/680 on the protection of natural persons with regard to the processing of personal data by competent authorities for the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties [2016] OJ L119/89 (Law Enforcement Directive).

[77] Case C-817/19 *Ligue des droits humains ASBL v Conseil des ministers* [2022] ECLI:EU:C:2022:491.

[78] For a similar point, Wilman (n 16).

unreasonable costs. The principle can be articulated as follows: *the state is only allowed to pursue digital enforcement in a targeted fashion; individuals shall not be placed under general suspicion that their behaviour or expressions are unlawful.*

5.5 The GMOP as a Harmonisation Tool

As a full harmonisation instrument, the DSA already leaves a small margin for national rules to impose due diligence obligations onto intermediaries to tackle illegal content online (see Chapter 17). But, even within that narrow space, the GMOP acts as a co-ordination mechanism for the Member States. Article 8 DSA stops the Member States from introducing various national experiments. Thus, for the digital single market, the robustness of the rule is crucial. It offers a general framework that limits national efforts to increase the responsibility of certain providers in their national law at the expense of harmonisation. It pre-empts uncontrolled national experimentation with policies that could undermine harmonised norms.

The GMOP is sometimes criticised by content industries for its inconsistency since providers are allowed to voluntarily do what the authorities cannot tell them to do. However, this criticism misses the point about the GMOP's legislative purpose. The GMOP, similar to liability exemptions, is a coordination mechanism. It constrains the Member States' ability to regulate. The GMOP limits the national legislatures directly. It does not limit providers who have the freedom to contract. The GMOP is instead a tool that dictates what type of monitoring behaviour, if requested by the state, shall be illegal. This explains why some types of monitoring cannot be requested by the Member States but can be adopted voluntarily by the providers or why some types of specific monitoring can be deployed by the EU legislation but not by the Member States.

This coordination role might have been overshadowed by the fact that the GMOP began to embody much more than just a framework for coordinating who can legislate in the zone of shared competencies between the Member States and the EU. The CJEU's interpretation of the concept, in conjunction with the EU Charter, means that some parts of the GMOP have obtained quasi-constitutional status—they cannot be legislated away even by the EU legislature.[79] As a result, some of the measures that are not allowed for the Member States to legislate on, cannot be introduced by the EU legislature either. Doing so would violate the EU Charter that protects the GMOP's core as a tool for balancing.[80]

[79] This is a part of the petrification effect that can also be observed in other parts of the EU law. Martin Husovec, 'Intellectual Property Rights and Integration by Conflict: The Past, Present and Future' (2016) 18 Cambridge Yearbook of European Legal Studies 239.

[80] *Poland* (n 8); *Scarlet Extended* (n 7).

From this perspective, there are two possible ways how to look at the GMOP:

- GMOP is a unitary *statutory provision* that always has the same meaning, regardless of whether it constrains the EU legislature and authorities or national legislatures and authorities.
- GMOP is a *principle* that has its core and *statutory versions*; while the EU legislature is bound only by the core guaranteed by the EU Charter, the Member States are bound by its statutory versions, which are left to the CJEU to interpret.

Under the second interpretation, only a core of the GMOP is guaranteed by the EU Charter and cannot be legislated away even by the EU legislature. The GMOP's statutory version in Article 8 DSA guarantees more protection than the core. It limits the Member States (and the EU) when introducing their measures in the area and the authorities interpreting them. The statutory scope is decisive when the CJEU reviews the actions of the Member States, particularly the orders of their courts or authorities (eg in cases of injunctions against intermediaries). The core, on the other hand, comes to its application when the EU legislature tries to undermine the GMOP itself. The EU legislature can fashion several versions of the GMOP as long as they comply with the core that is guaranteed by the EU Charter.

The gap between the core and statutory versions of the GMOP determines to what extent the EU can implement something that its Member States cannot.[81] This sounds odd, but it would be consistent with the harmonisation logic behind the provision. It explains why the EU's legislative instruments, such as the CDSM Directive, can adopt different approaches regarding liability while still reiterating that they follow the principle.[82] In such areas with specific laws, the EU legislature complies with the core of the principle, but not necessarily with a specific statutory version (eg Article 8 DSA) that is binding upon the Member States.

Under the first interpretation, on the other hand, the GMOP has a single meaning, which is the same for the Member States' legislatures and the EU legislature. Measures imposed by the Member States are constrained identically to those imposed by the EU

[81] AG Øe argued the opposite that there is no gap. He states that 'the concept of 'general monitoring obligation' must be interpreted in the same way, irrespective of the origin of such an obligation'—ie whether it is a national or an EU measure: *Poland (Opinion of AG Øe)* (n 37) fn 124.

[82] Some emphasise that even art 17 CDSM Directive remained under art 15 ECD, and thus, the meaning should remain the same. In my view, if the context changes, the meaning can too, and while technically correct, I do not necessarily think that the concepts used in two different contexts retain the same meaning.

legislature. It also means that even where Article 8 DSA does not apply, the GMOP still follows any EU legislation as a shadow.[83]

Case law to date does not give a satisfactory answer to this very consequential question. The only case to date that could have clarified the issue, *Poland*, failed to do so. When discussing two different directives that mention the GMOP, the Court noted that they express the GMOP in 'similar terms', thus suggesting that they could express it in principle. When the Court applied the concept, it spoke about it as 'an additional safeguard', then interpreted as limiting the use of automation.[84] This latter remark would suggest that the GMOP can mean different things in different legal acts, and its content might be influenced by other safeguards in each specific legal act.

In my view, it is too early to tell. Given the legislative history and purpose, the second interpretation appears to me to be more plausible. The GMOP was initially only mentioned in Article 15 ECD. However, the references to it in the meantime have been added to many other acts, such as the General Data Protection Regulation (GDPR), Audiovisual Media Services Directive, CDSM Directive, and the Terrorist Content Regulation.[85] The GMOP has indeed become a key principle of internet regulation, whether directly or by cross-reference to Article 15 ECD. In the coming years, the GMOP as a constitutional and statutory concept (in Article 8 DSA or other acts of EU law) will likely gain even more importance.

In my view, given the rising number of EU legislative acts, the CJEU will have to clarify at some point that the use of the concept means different things in different contexts, for instance, in the constitutional context (as a brake on legislature) and the statutory context (as a feature of diverse legislative solutions). It is plausible that soon the Court might recognise several legislative designs of the GMOP, with Article 8 DSA offering the baseline meaning from which other acts can deviate if they offer more extensive complementary safeguards.

For instance, one could argue that when Article 17 CDSM Directive imposes a stay-down obligation that entails filtering, *its* GMOP is informed by the effectiveness of other legislated safeguards mitigating the same risks. This means asking: what did the EU legislature additionally do to contain these risks in this specific setting? If the legislature took the risks into account, then arguably, the specific version of the GMOP standard in a separate legal instrument could be more permissive, as in *Poland*. The reason is that the relevant concerns are now partly addressed by more specific safeguards in the statutory design (eg prior risk assessment).

[83] The best example to date is the CJEU's transplantation of the GMOP into the IP Enforcement Directive, including in the offline context: see *Tommy Hilfiger* (n 31) para 34. For more on the debate, Husovec, 'Holey Cap! CJEU Drills (yet) Another Hole in the e-Commerce Directive's Safe Harbours' (n 12) 118ff.

[84] *Poland* (n 8) para 90.

[85] Audiovisual Media Services Directive, Rec 48 and arts 28a(5), 29b(1), and 29b(6); CDSM Directive, Rec 66 and art 17(8); Terrorist Content Regulation, Rec 25 and art 5(8). For its precursors, see the General Data Protection Regulation, Consumer Protection Cooperation Regulation, European Electronic Communications Code Directive, Market Surveillance Regulation, General Product Safety Regulation and Payment Services (PSD2) Directive.

If the Court admits such split reading, the guiding principle should be the risk of abuse of such monitoring. When the European legislature departs from the DSA, it must still calibrate its interventions well to address the core concerns of indiscriminate monitoring. With this reading in mind, the Court's reference to the GMOP as an 'additional safeguard' in *Poland* paints it as a sort of a backstop safeguard—the internet's ultimate safety net.[86] Put differently, Article 8 DSA is a default rule of the legal system that only the EU legislature can redesign, but never suspend entirely. It is a pillar of the DSA as a digital rights charter (see Chapter 18).

5.6 The GMOP vs the Member States

Liability exemptions require that specific monitoring must be administered by authorities or courts on the national level (see Chapter 8). In the absence of EU legislation dispensing with this requirement, specific monitoring based on mere requests of individuals violates the DSA. But the problem is that assurance of the proper scope of such orders often requires more procedural safeguards, such as rights to affected parties to challenge implementations (*UPC Telekabel*),[87] or the need for oversight of the implementation (*Glawischnig*).[88] However, the doctrine of procedural autonomy of the Member States somewhat limits the ability of the CJEU to demand specific procedural safeguards. According to the settled case law:

> in the absence of EU rules on the matter, it is for the national legal order of each Member State to establish procedural rules for actions intended to safeguard the rights of individuals, in accordance with the principle of procedural autonomy, on condition, however, that those rules are not less favourable than those governing similar domestic situations (principle of equivalence) and that they do not make it excessively difficult or impossible in practice to exercise the rights conferred by EU law (principle of effectiveness)[89]

Given that most EU law does not introduce such safeguards, it is unsurprising that the national situation is far from ideal. For instance, Austrian and German courts narrowed down the procedural safeguards following *UPC Telekabel*'s ruling to a theoretical ability to sue in a separate lawsuit.[90] German and Austrian courts

[86] Graham Smith makes a similar point, Graham Smith, 'Time to Speak up for Article 15' (*Cyberleagle*, 21 May 2017) <https://www.cyberleagle.com/2017/05/time-to-speak-up-for-article-15.html> accessed 1 August 2023.
[87] *UPC Telekabel* (n 8) para 57.
[88] *Glawischnig* (n 7).
[89] Case C-3/16 *Lucio Cesare Aquino v Belgische Staat* ECLI:EU:C:2017:209, para 48.
[90] Austrian Supreme Court case OGH 24.06.2014, 4 Ob71/14s, para 5.1; the Hamburg District Court case, LG Hamburg v 12 May 2021 – 310 O 99/21. <https://www.quad9.net/uploads/20210618_Sony_Quad9_Injunction_GERMAN_redact_ccaba9768b.pdf> accessed 1 August 2023.

have also interpreted the GMOP as permitting obligations to filter that involve humans.[91]

Without further specification of the safeguards, the effectiveness of Article 8 DSA is heavily limited by the consequences of the doctrine of procedural autonomy. This comes at the expense of the rights of some individuals. In this context, Kaleda, a judge of the General Court, argues[92] that '[i]n the absence of harmonisation, the application of Article 47 of the Charter could therefore lead to the establishment of a minimum procedural standard, which can be invoked in order to achieve a certain degree of uniformity'. This is particularly important for some injunctions where the two litigating parties neglect the position of the affected third party—the so-called 'Three-Body Problem'.[93]

Apart from Article 47 EU Charter, another solution is to strengthen the quality of the law analysis. The CJEU could require that safeguards be adopted explicitly *by legislation*. After all, the EU Charter and Court's case law dictate that the interference and safeguards must be 'prescribed by the law'.[94] Since Article 8 DSA already acts as a coordination tool by giving the Member States permission to intervene by imposing specific monitoring, it only makes sense to require that permitted measures are safeguarded against abuse *explicitly* within national legislation. Thus, any acceptance of website blocking, for instance, would only be possible if national law also spells out the safeguards that the Court prescribes.

The English courts have demonstrated the most elaborate thinking about safeguards in European case law. They require discharge clauses in cases of a material change, and for the benefit of targeted websites and affected providers, transparency notices to the public and explicit sunset clauses.[95] This is in stark contrast with some other jurisdictions that sometimes do not foresee any safeguards at all.[96]

[91] *Alone in the Dark case* (n 23), where this was first accepted by the German Federal Supreme Court; Austrian Supreme Court case, OGH 4 Ob 36/20b (n 49) para 6.1.

[92] Saulius Lukas Kalėda, 'The Role of the Principle of Effective Judicial Protection in Relation to Website Blocking Injunctions' (2017) 8(3) Journal of Intellectual Property, Information Technology and Electronic Commerce Law 216; also discussion of the procedural side in Martin Husovec, 'Injunctions against Innocent Third Parties: The Case of Website Blocking' (2013) 4(2) Journal of Intellectual Property, Information Technology and Electronic Commerce Law 116.

[93] Daphne Keller, 'The Three-Body Problem: Platform Litigation and Absent Parties' (*Lawfare*, 4 May 2023) <https://www.lawfaremedia.org/article/the-three-body-problem-platform-litigation-and-absent-parties> accessed 10 August 2023.

[94] *Poland* (n 8) para 67; also Case C-311/18 *Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems* ECLI:EU:C:2020:559, para 176; *Opinion 1/15 of the Court (Grand Chamber)* ECLI:EU:C:2017:592, paras 140–41.

[95] *Cartier International AG & Ors v British Sky Broadcasting Ltd & Ors* [2014] EWHC 3354 (Ch) [262].

[96] To illustrate the state of fragmentation, the website blocking injunctions are subject to many different national practices regarding the following issues: (a) who is considered to be an infringing third party, (b) the form of the orders, (c) their specificity, (d) scope of preventive duties, (e) types of used technologies, (f) possibility of ex post submission upgrade, (g) use of a subsidiarity principle, (h) assessment of effectiveness, (i) cost allocation, (j) post grant supervision, (k) locus standi for users and website operators, and (l) the enforcement of court orders. See Martin Husovec and Lisa van Dongen, 'Website Blocking, Injunctions and Beyond: View on the Harmonization from the Netherlands' (2017) 12(8) Journal of Intellectual Property Law & Practice 695.

In my view, expecting civil judges to introduce such safeguards in their orders is unrealistic. Post-DSA, the advantage is that many horizontal safeguards will already be introduced; however, not all of them will apply to compliance with national orders. Ideally, the Member State (or the EU) should adopt more detailed national legislation about how injunctions against intermediaries are to be handled by courts, what safeguards can be imposed by courts or supervised by other authorities, and who should carry what costs. The Member States that rely on administrative enforcement of orders already do it to some extent. However, more horizontal laws of this type are generally missing.