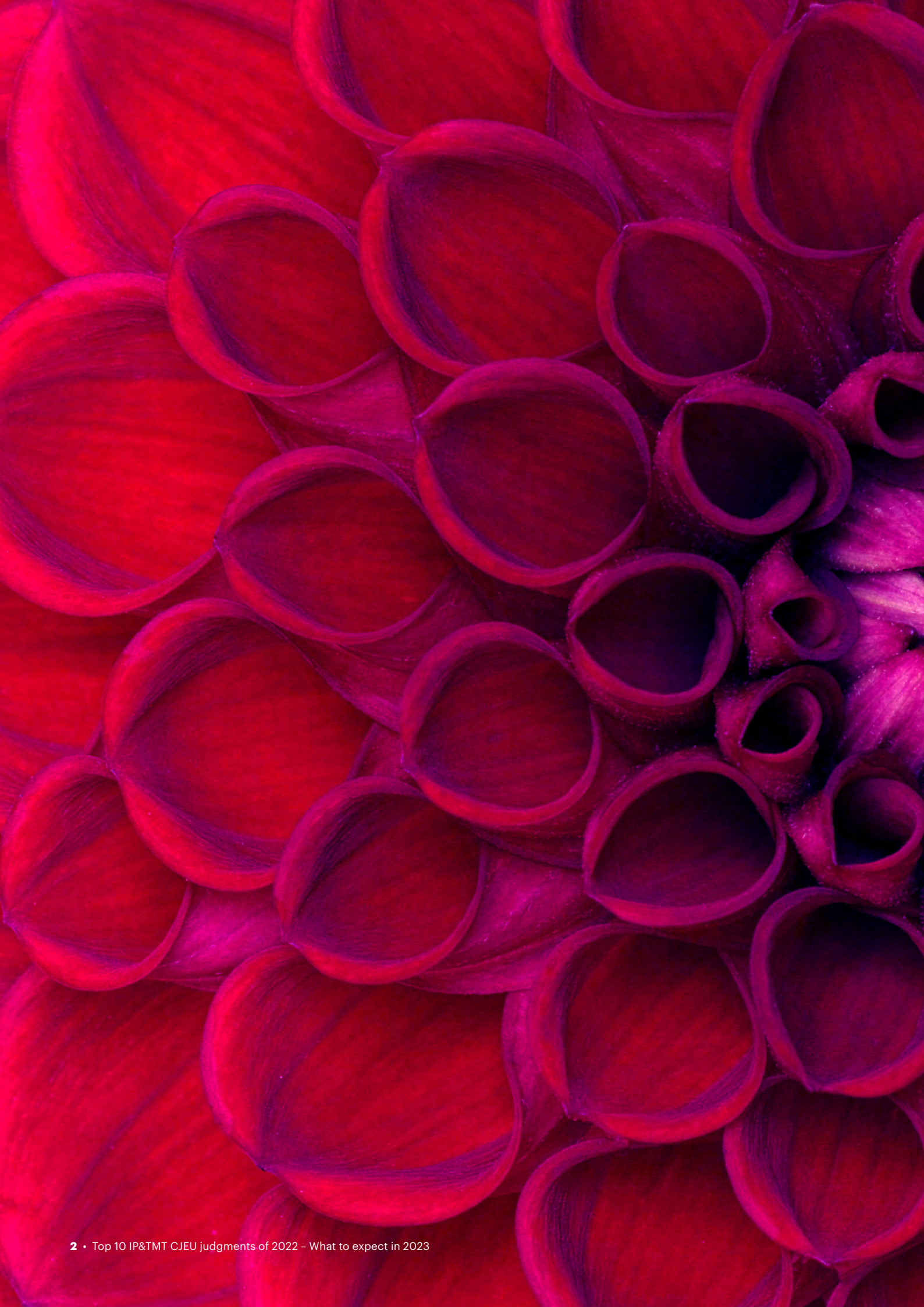
大成 DENTONS

Top 10 IP&TMT CJEU judgments of 2022

What to expect in 2023

Grow | Protect | Operate | Finance

March 2023



Introduction

Karol Laskowski
Europe Co-head of Technology, Media and Telecommunications

Last year brought a number of crucial CJEU judgments that directly affect the data protection, TMT and intellectual property domains. The new decisions have impact on how this sector's companies will apply the existing laws but may also give rise to new, sometimes more demanding, obligations. Mindful of the difficulties business operators in this field may encounter, not least due to the slew of CJEU rulings, Dentons has compiled a list of ten CJEU judgments which, in our view, might be of significance for your work outcomes.

The third edition of our report covers decisions affecting the three fields specified above. Notably, our short analysis clearly shows that much work and thought was put into the sphere of data protection last year. The CJEU has delivered numerous judgments specifically related to personal data that can only be taken as a sign of just how dire the need is to further explain and interpret some particular issues.

Although each and every case included in the report significantly affects European law, we consider the dispute between Poland and the EU Parliament to be especially interesting and decisive. Due to that, the judgment which imposes an obligation on internet search engines to filter potentially infringing content stands as number one on our list. The case has given rise to numerous controversies and questions on proportionality of that requirement. Nevertheless, the judgment is clear on how search engine platforms ought to perform their tasks from now on.

The other two places on the podium have been taken by the SpaceNet case and RTL Television. The first one touches upon the issue of traffic and location data retention in the context of telecommunications providers. RTL Television once again discusses the problem of transmission of television programs in hotel rooms but this time the focus was on the conceptual autonomy of the cable retransmission and the extent to which broadcasting organizations have the right of communication to the public.

Following that, we have decided to include some particularly important cases in the field of data. The next judgments revolve around issues such as data storage, either for creating error-detection databases or in the context of market-crime detection, cloud services as well as processing personal information of an especially sensitive nature. Apart from that, three cases adhering to intellectual property laws have been discussed. Austro Mechana and Koch Media both address questions referring to copyright and related laws. Last but not least, one judgment of the General Court, which in our opinion deserves some attention and might be especially interesting for trademark law specialists, has been ranked tenth in our list.

.

Poland vs the European Union Parliament and Council

1

C-401/19

#theDSMDirective #freedomofexpression

Background

Poland filed a complaint against the European Parliament and the Council of the European Union seeking annulment of Article 17(4)(b) and Article 17(4)(c) in fine of Directive (EU) 2019/790 of the European Parliament and of the Council of April 17, 2019 on copyright and related rights in the digital single market and amending Directives 96/9/EC and 2001/29/EC, alternatively, to annul that Article 17 in its entirety, in the event that the Court finds that those provisions cannot be severed from the other provisions contained in Article 17 of Directive 2019/790 without altering the substance of the regulation contained in that article.

The Directive provides for a liability exemption mechanism for Online Content Sharing Service Providers ('OCSSPs) which is available only after specific conditions are met. Requirements included obtaining an authorization, ensuring unavailability of specific protected content and putting in place a notice and take down/ stay down procedures. The main issue was that the provision, called also a "value gap" or "upload filter", imposes a new liability regime for user-generated content sharing platforms, intended to review the uploaded content. As the scale and difficulty of the task is unquestionable, content filtering and automatic recognition is the only possibility to ensure a liable review and consequently, compliance with "best efforts" imposed on platforms by the Directive. Poland, which contested article 17, argued that this amounts to the necessary introduction of measures that are preventative in nature and impose strict control over the published content. The main point was that, according to Poland, such requirements do not comply with the right to freedom of expression and that it lacks proportionality.

Judgment

The Court, in the judgment, rejected Poland's complaint with regard to the main claim and dismissed the remaining part.

The Court held that the obligation imposed on online content service providers to verify the content have been surrounded by adequate safeguards by the Union legislature to ensure respect for the right to freedom of expression and information of users of these services and a fair balance between, on the one hand, this right and, on the other hand, the intellectual property right protected under Article 17(2) of the Charter.

In its ruling, the CJEU weighted different rights and freedoms against each other. It confirmed that article 17 does impose an obligation on the de facto filtering of content where necessary and relevant information has been provided by the rights holders. According to the Court, the need for protection of intellectual property rights requires that a certain limitation of expression and information is imposed on the right of an internet user. However, it also notes that such limitation is justified as property rights require proper protection and effective measures that would ensure respect of fundamental rights as that of ownership. The Court also emphasized that such protection can only be possible in a complicated digital environment where automatic filtering measures are deployed. Nevertheless, the CJEU argued that such measures have to be taken to make a distinction between lawful and unlawful content or else they would not be in line with the requirements of article 17. Next, the general exceptions applicable to intellectual property rights, such as parody or pastiche, are to be respected and allowed. The judgment also underlined those obligations stemming from this disputed provision

are not meant to create any monitoring regime on the OCSSPs and it only serves as an additional safeguard, protecting the property rights of their holders. Likewise, providers cannot be subject to any content publication prevention measures and remain free to offer their services so that the public can show and access various pieces of information and work online.

Experts' comments

Karol Laskowski

It is not surprising that article 17 of the DSM Directive raises controversies within the legal environment. The provision imposes a rather strict liability regime on the online content sharing service providers, which may seem problematic in the context of principles such as freedom of expression and information. Nevertheless, in these times, when countless online copyright breaches are in evidence, there is a true need for regulatory mechanisms capable of imposing at least some degree of control.

What I find to be particularly interesting about this case is the emphatic need for automatic recognition and filtering tolls. Enabling such solutions by the OCSSPs' seems to indeed be the only feasible way to ensure compliance with the new law, that at the same time is not overly arduous or simply impossible to conduct. Nevertheless, the judgment is silent on any specific rules and guidelines on how filtering tools should be deployed. The one clear requirement is that fully automated upload filters can only be able to block content which the court has already found to be infringing or one that is manifestly unlawful. In comparison to the elaborated opinion of the Advocate General, this is not enough and much more detail could have been provided by the CJEU so that the businesses affected by the new obligation know how to correctly implement it to their services. The same holds true for the enforcement of users' rights. The complaint mechanism enshrined in the Directive and dispute-settlement processes may prove to be inadequate safeguards for users and much more could have been said in that regard.

Given the above, I suspect that this case is not the last one when it comes to article 17 of the DSM and the future will bring more disputes and hopefully also clarifications on that matter.

Małgorzata Domalewska

It is difficult not to share the Court's position. The absence of the provisions challenged by Poland would in principle change nothing in terms of the protection of authors in relation to the existing provisions under Article 14(1) of Directive 2000/31. Online content sharing platforms are an increasingly common source of access to content, but unfortunately also largely made available illegally. Article 17 of the DSM Directive, while introducing a new liability regime, at the same time ensures that the principle of proportionality is upheld, referring to it literally in paragraph 5. It also introduces a number of limitations, explicitly indicating, for example, the assurance of the continued use of exemptions and limitations such as the quotation or criticism. It is also important to note that the obligation to prevent future unlawful sharing of protected subject matter applies only to works for which providers have information on their infringement.

As a side note, it is worth noticing that the Polish draft law appears to correctly implement Article 17 of the DSM Directive. However, doubts may be raised by the proposed provisions indicating that a service provider cannot be required to prevent access to a work, block access to a work or remove a work if making it available to the public does not obviously and indisputably infringe copyright. In principle, any posting of a work about which a right holder raises objections will, by its very nature, be contentious. The words "in an obvious and indisputable manner" added in the Polish draft, may lead to the illusory nature of the new solutions that were supposed to implement the Directive.

SpaceNet

C-793/19

#ePrivacy #trafficdata

#telecommunicationsproviders

2

Background

SpaceNet, a German Internet provider who sued the Federal Republic of Germany litigated in a case concerning the requirement to store telecommunications traffic data of its clients. German Telecommunications law imposed an obligation for an indiscriminate ten-week storage period of telephone and internet connection data by phone and Internet providers in case they could aid in law enforcement investigations. SpaceNet argued that such provisions are contrary to the GDPR, especially the principle that any person other than the users is prohibited from storing, without the consent of the user concerned, the traffic data related to electronic communications. Another argument raised was that such storing does not comply with the requirement under Article 6 of the GDPR according to which the processing and storage of traffic data are permitted only to the extent necessary and for the duration necessary for the billing and marketing of services and the provision of value-added services. The referring Court did not agree with SpaceNet, arguing that it believed the German rules concerned fewer data and a shorter retention period. Due to that, the Court's view was that the national telecommunications law offered an adequate level of protection for individuals against possible infringements of their privacy and data protection rights.

Judgment

Firstly, the CJEU ruled that the provisions of the ePrivacy Directive preclude national laws which oblige providers of electronic communication services to retain traffic and locations data of their subscribers and registered users which relates to the activities of this service for the purpose of crime prevention. Second, the Court added that the data in question, especially with regard to its diversity and quantity, is capable of revealing quite precise details about a person's private life and thus, even short retention periods are a danger to fundamental rights to privacy. Following that, the Court also noted that, with regard to the safeguards implemented for the protection of the stored data, distinction should be made between access to data and its retention, as the two constitute two separate legal matters. As such the mere fact that data is being retained is in itself a problematic aspect in the light of the GDPR provisions, without consideration for how it can be accessed and under what conditions.

Nevertheless, the Court also emphasized that the relevant rules of the ePrivacy Directive cannot diminish the effect of national laws which aim at safeguarding national security or combatting serious crime. Specifically, EU privacy rules should preclude national provisions which regulate retention of traffic and location data when a serious threat to national security is present and apparent. Additionally, a limited and targeted retention of such data, general and indiscriminate retention of IP addresses or data revealing the civil identity of the electronic communication service users and, lastly, the expedited retention of traffic and location data after a specific instruction by a competent authority, can be justified and allowed. Regardless of the above, conditions ensuring the safe retention of data in question and safeguards for the data subjects should be respected and in place.

Experts' comments

Paweł Gruszecki

Significantly, the judgment in this case introduced a clear division into specific cases of retention of particular categories of data (i.e. traffic and location data, IP addresses assigned to the source of an internet connection, and data relating to the civil identity of users of electronic communications systems) according to the intended purpose of the retention.

Therefore, a distinction is made between the cases of the above data and the allowed activities that may be permitted in their respect by national laws. The permissibility of retention, including its conditions, of the above data is therefore different depending on whether it is for the purpose of: (i) safeguarding national security (the civil identity of users of electronic communications systems, IP addresses, traffic and location data) or (ii) combating serious crime and preventing serious threats to public security (IP addresses, traffic and location data); (iii) combating serious crime (traffic and location data); (iv) safeguarding national security in situations where the EU member state concerned is confronted with a serious threat to national security that is shown to be genuine and present or foreseeable (traffic and location data) and (v) combating crime and safeguarding public security (civil identity of users of electronic communications systems). Surely, national legal measures that provide, on a preventive basis, for the purpose of combating serious crimes and preventing serious threats to public safety, for the general and non-discriminatory retention of traffic and location data, are not permitted.

Given its comprehensive approach, it is hoped that the judgment has been studied in detail by EU member states that have been working to implement the European Electronic Communications Code (EECC) into national legislation, resulting in significant changes to the regulation of the electronic communications sector.

Bartosz Dobkowski

Following the invalidation of the Data Retention Directive (2006/24/EC), EU Member States have resorted to Article 15(1) of the ePrivacy Directive to justify national legislation measures aimed at the retention of traffic or location data for purposes related to the protection of public security, defence, state security and the enforcement of criminal law.

Throughout the years, the CJEU developed a detailed position on such measures, in particular in its judgments in Tele2 Sverige AB v Post (Joined Cases C-203/15 and C-698/15), Ministero Fiscal (C-207/16), La Quadrature du Net (Joined Cases C-511/18, C-512/18 and C-520/18) and G.D. v The Commissioner of the Garda Síochána (C-140/20).

In SpaceNet, the CJEU has confirmed that the EU law, in particular the ePrivacy Directive, precludes national legislation prescribing, for the purposes of combating serious crime and preventing serious threats to public security, the general and indiscriminate retention of data. However, Member States may, with the aim of combating serious crime and strictly respecting the principle of proportionality, provide for e.g. the targeted or expedited retention of such data as well as generalized and undifferentiated retention of IP addresses.

The judgment in SpaceNet provides a clear guidance to EU Member States and shows that the exclusion of certain means of communication or certain categories of data and the limitation of the retention period may not be sufficient to eliminate the risk of establishing a comprehensive profile of the persons concerned and may not justify the general and indiscriminate retention of data by telecommunications (electronic communications) service providers.

It will be interesting to see how Member States will approach the above judgment taking into account that data retention regimes in some of them still rely on the annulled DRD and are not compliant with the subsequent case-law.

RTL Television

C-716/20

#InfoSoc #cableretransmisison #copyright

3

Background

RTL Television GmbH ("RTL") is a broadcaster of free-to-air channels whose private reception is not subject to a license fee. The signal of RTL was captured by one of the Portuguese hotel operators and offered in hotel rooms after a retransmission via a coaxial cable connected to televisions. As it was made available without prior authorization, the broadcaster requested adequate compensation for retransmission in the hotel rooms. The hotel operators of Grupo Pestana S.G.P.S. SA and SALVOR – Sociedade de Investimento Hoteleiro SA, the defendants, argued that according to the relevant national law, hotels were exempted from copyright fees when receiving a TV signal. The first instance Court and subsequently the appeal Court both agreed that where a signal distributed from an RTL Channel to hotel rooms would normally be considered a public communication act and constitute a retransmission of broadcast, it cannot be regarded as such in the present case because the hotels in question are not broadcasting organizations. As the rights in question are governed by multiple legal documents, namely the SatCab Directive, InfSoc Directive and the laws adopted on the national level, it was hard for the Court to determine whether the claims of the broadcaster should be decided on the basis of the right of communication or perhaps the more specific regime dictated by the Sat/Cab Directive.

Judgment

Although cases about the transmission of radio television programmes in TV sets installed in hotels have already been adjudicated by the CJEU, they touched upon slightly different issues. In the case at hand the main questions concern the conceptual autonomy of the cable retransmission as a broadcaster's right and SatCab Directive. The court referred to EU law guaranteeing exclusive rights in favour of broadcasters. It pointed, inter alia, to Directive 2006/115, which guarantees broadcasters the right to authorise the wireless retransmission of its programmes and the communication to the public of its programmes when such communication is made in places accessible to the public against payment of an entrance fee. The court also referred to the case law confirming the possibility to grant more far-reaching protection than under Directive 2006/115. With regard to the SatCab Directive, the Court underlined the SatCab Directive's objective to facilitate, on the one hand, satellite broadcasting and, on the other hand, cable retransmission, promoting the authorisation of cable retransmission by authors and holders of related rights through collecting societies. The Court emphasised that the SatCab Directive is not intended to affect the scope of copyright and related rights as defined by EU law and the laws of its Member States. The SatCab Directive does not grant broadcasters any exclusive right to authorise "cable retransmission", and facilities such as a hotel are not covered by the concepts of "cable network operator" or "cable operator" within the meaning of Directive 93/83.

Experts' comments

Karol Laskowski

The case at hand constitutes yet another dispute concerning the transmission of television programmes in hotel rooms but this time the issue narrows down to the very notion of "cable retransmission". The judgment is particularly significant as it interprets the interplay between the relevant EU laws of the InfoSoc Directive and the SatCab Directive in more detail. I find that the well-established system in which copyrights are collectively licensed to the hotels by the collecting societies to be a well-functioning, rehearsed system that benefits all the involved parties and makes the process smooth and clear. Were the Court to rule otherwise, this system could collapse and cause unnecessary complications, even for hotels whose win could be perceived as beneficial only on the surface. Furthermore, the retransmission refers to a specific technology that the SatCab Directive meant to regulate and that is only made by professional cable networks. Thus, I agree with the findings of the Court, as well as the Advocate General's opinion, according to which retransmission such as one done by the Pestana Group cannot be regarded as one specified in the Directive.

Małgorzata Domalewska

This is another ruling concerning the making available of television programmes to hotel guests. This time, the Court considered the issue of broadcasters' related rights to retransmit programme signals by hotels in the context of the SatCab Directive. The Court rightly pointed out that the SatCab Directive does not impose an obligation on Member States to guarantee broadcasters an exclusive right to authorise "cable retransmission" (the purpose of the Directive is different), and that such retransmission by a hotel does not constitute cable retransmission within the meaning of the Directive. On the other hand, notwithstanding the SatCab Directive, the possibility for Member States to grant such exclusive rights to broadcasters within their legal orders cannot be excluded. According to the case-law cited by the Court in the RTL case, in C More Entertainment, C 279/13, the court confirmed that Member States may grant broadcasters the exclusive right to authorise the communication to the public of their broadcasts under conditions which differ from those provided for in Article 8(3) of Directive 2006/115.

Digi

Case C-77/21

#purposelimitationprinciple #gdpr #dataprocesing

4

Background

Digi, a leading internet, and TV service provider in Hungary, was heavily fined for alleged infringements of article 5(1)(b) and 5(1)(e) of the GDPR, as well as various data security requirements. The penalty was imposed mainly due to the prolonged storage of around 322 thousand consumers data in a database created for test purposes after an "ethical hacker" managed to access the system and significant amounts of personal information. Digi corrected the error which allowed this unlawful access, deleted the database and notified the Hungarian Supervisory Authority ("NAIH") about the breach. NAIH decided to impose a fine because, according to their reasoning, the database had been initially created for a different purpose than the one for which the customer's data was excessively stored for almost 18 months. Following that, Digi challenged the lawfulness of the Authority's decision, and the matter has been brought before the Hungarian Court. Due to further uncertainties around the correct understanding of the relevant GDPR provisions, two questions have been referred to the CJEU, namely: whether the copying of data to another internal database which were collected for a limited purpose changes the purpose of collecting and processing the data and whether the fact of creating a test database (i.e., keeping data collected for a limited purpose in another internal system) and continuing to process the data in that way is compatible with the purpose of collecting the data.

Judgment

In its decision, the Court confirmed that data of Digi consumers had been initially collected in a lawful way for the purposes of entering and performing subscription contracts. The issue arose when data was moved to a different database as this constitutes "further processing" in the meaning of the GDPR. According to the judgment, in order to determine whether the first established purpose is compatible with the subsequent one, account must be taken to aspects such as the existence of possible link between the two purposes, the context of data collection, the nature of the processed data, potential consequences of the processing and the adequate safeguards in place for both processing operations. In relation to the above, the conclusion to the first referred question was that article 5(1)(b) GDPR does not preclude the recording and storage by the controller in a database created for the purpose of carrying out tests and correcting errors, of personal data previously collected and stored in another database, where such further processing is compatible with the specific purposes for which the personal data were initially collected, which must be determined in the light of the criteria set out in Article 6(4) of that regulation.

As per the second question, the Court notes that personal data must be retained in a form which allows the identification of data subjects for no longer than is necessary for the purposes for which they are processed. Further, it confirms that it is for the controller to demonstrate that data is being held only for period necessary to achieve the objectives of the processing. Personal information stored for longer than that period, even if for the same purpose as set initially, would not be in line with the applicable law and thus, should be destroyed. The Court also underlined the importance of ensuring that data processing is performed with respect to the data minimisation principle and, where no consent has been given, with the necessity requirement. Moreover, lawful processing ought to be done in a secure way which provides high level protection for the natural persons concerned. Digi failed to delete data from the database after the test and error correction had been carried out and thereby violated article 5(1)(e) of the GDPR.

Experts' comments

Aleksandra Danielewicz

There are three important takeaways from this judgement. The first is that purpose and storage limitations have various functions. The latter serves the other principle of data minimization to preserve personal data privacy while also reflecting the proportionality principle in a temporal sense. Even if there are concerns regarding the storing of personal data in excess, this does not necessarily mean that the processing itself breaches the principle of purpose limitation. The second and more practical takeaway is that the data controller can temporarily store personal data in an alternative database in the event of a technical malfunction or cybersecurity incident in order to fulfil its obligations regarding personal data security, such as maintaining personal data availability (Article 32 of the GDPR). To justify the additional processing, there is no requirement to rely on a different justification. And the third takeaway is that data controllers do not retain personal information excessively if they create an additional database to ensure its accessibility in the event of a technological breakdown. They ought to remove private data from the second database as soon as the issue is resolved.

Paulina Węgrzynowicz

What is important in this judgment is, first of all, that the CJEU underlined the importance of Article 6(4) of the GDPR in the case of processing of data for purposes other than for which the data was primarily collected in order to fulfil the GDPR's the principle of purpose limitation. It might be interesting to see whether the controllers, in order to process the data for such supplementary purpose, would have to somehow document that they had considered the conditions set out in Article 6(4). What is more, the CJEU stated that even if the other purpose is compatible with the one for which the data was collected, it does not justify storing the data for longer than necessary for this other purpose.

Austro-Mechana

C-433/20

#cloudcomputing

#faircompensation

5

Background

This case tackles the private copying exception and the compensation for the reproduction and storage of copyright material in a cloud. Austro Mechana, a copyright collecting society, collects the remuneration for the exploitation of the right of reproduction on storage media. Austro-Mechana sued Strato, a German company, which offers a service to customers providing cloud computing storage. Austro-Mechana's claim was based on the assumption that the remuneration for exploitation of the right of reproduction on storage media is payable where storage media of any kind are "placed on the market" – by whatever means and in whatever form – within national territory, including the cloud-based storage spaces. Strato, on the other hand, argued that the Austrian copyright law regulating remuneration in such cases does not extend to cloud services and emphasized that its users have already paid the copyright fee while acquiring devices which allow access to the cloud-stored content. The Court of First Instance ruled in favour of Strato as according to its reasoning, Strato does not offer storage media, as defined by the relevant Austrian law, but merely makes the storage capacity available. Austro Mechana decided to make an appeal and the subsequent court referred the issue to the CJEU.

Judgment

The first question asked of the CJEU concerned the private copying exception and whether cloud computing falls within that notion even where it was made available only for private use. The CJEU concluded that Directive 2001/29 should be read broadly and ensure a high level of protection for authors. Thus, the answer was given in the affirmative, confirming that cloud computing is also addressed by the provisions of Directive 2001/29 without relevance to the ownership of the servers on which such service is based.

With regard to the second question which concerned the issue of whether Directive 2001/29 precludes national law implementing private copying exemption but not requiring the storage service providers to pay fair compensation, the Court concluded that Member States are not required to demand fair compensation for such services. However, in situations of this kind, such compensation ought to be paid to the right holders by a different route. In this case a levy on equipment that was paid by the users was seen as enough and deemed acceptable. Thus, Member States have a degree of discretion when it comes to deciding on how such compensation is to be made. The judgment underlined those national laws should ensure that the compensation paid does not exceed the possible harm to owners of intellectual property rights that result from acts where multiple devices are included in a process.

Experts' comments

Aleksandra Politańska-Kunicka

Current cloud services are popular storage devices and it is important that they are addressed by the law on copyright. Treating cloud computing as a private copying exception, even when done for private use, gives authors the needed protection for their works. The Court correctly pointed out that fair use reproduction, which does not make the work available to the public, also includes storing by cloud computing service. The Court also rightly underlined the need to maintain a balance between different interests and take into account the actual harm of copyrights holders.

Kamil Januszek

This ruling addresses an important issue of the rules of introducing reproduction levies with respect to the private copying exemption using cloud computing services. Without a doubt, in line with the wording of Directive 2001/29, private copying exemption requires an equitable financial compensation towards the right holders payable one way or another by the entities which in fact carry out the cloud storage i.e., the end users (not the providers). The Court rightly considered the specific nature of the cloud storage services and related difficulties in identifying all end users obligated to pay such compensation. Therefore, the Court's solution of a discretional character for each Member States' competence of collecting such compensation, seems to be sensible e.g., via a system of a private copying levy chargeable to the producer or importer of the servers on which the cloud storage is being carried out by the end users. That levy would ultimately be passed on economically to the private user who uses that equipment or to whom a final reproduction service is provided. Finally, the Court also rightly underlined that the amount paid via the above levy must take into account and should not exceed the possible harm borne by copyright holders due to private copying

Tímea Bana

The Court of Justice of the European Union has concluded that the saving, for private purposes, of copies of works protected by copyright on a server provided by a cloud computing service provider, should be included to the private copy scheme. However, the CJEU did not examine the legitimacy of the private copying levy in the era of streaming and whether or not, the level of compensation for the alleged harm suffered by the copyright holders with respect to media storage capacities is fair and interconnected. The private copying levy schemes were introduced in certain jurisdictions and Europe-wide to compensate copyright holders for the damage caused by private copying (in particular private copying of cassettes and CDs) in the analogue era, which was highly widespread in the 1980s and 1990s. Nowadays, however, consumption habits have changed dramatically and typically, end-users no longer consume works by copying them, but mainly through streaming platforms. Today, storage media, including cloud services, do not primarily contain works of third party (copyright) rightsholders, but private content, documents and private photographs. Therefore, I expect that many new court cases will attempt to challenge the legitimacy of the level of compensation for copyright holders as private copying levies must be linked to the harm suffered by the rightsholders resulting from copies made for private use.

VD and SR
C-339/20 and C-397/20

6

Background

VD and SR were two suspects accused of insider dealing, concealment of insider dealing, corruption and money laundering by the French Financial Markets Authority ('AMF'). French legislation allows authorities such as the AMF to request operators providing electronic communication services to transmit traffic data connected to phone calls in order to investigate potential market crimes. After the collection of data from operators, the AMF initiated its investigations against the two data subjects. Following that, the suspects challenged the use of the data by the Authority, arguing that its collection was not in compliance with the relevant EU law. Additionally, a second issue was raised which concerned the lack of any restrictions regarding the powers of AMF investigators to collect the data retained by the operators. The French Court hearing the case was unsure whether the existing French legislation was in line with the EU rules. Despite the fact that the European law provides for situations where traffic data has to be accessed for investigatory purposes, the Directive on privacy and electronic communications restricts the retention of data and contradicts the anti-market abuse rules. The court of cassation was unsure how to balance the requirement imposes by the divergent laws and thus, referred preliminary questions to the Court of Justice of the European Union.

Judgment

First, the European Court ruled that the law on Market Abuse does not impose obligations on the operators providing electronic communication services to retain the gathered data. Thus, there is no valid legal basis stemming from the Market Abuse laws to keep the data by those providers for the purpose of enabling the competent authorities to investigate and fight the financial abuses. Although the Directive on privacy and electronic communications does govern such instances, the case law on this matter clearly indicated that the general and indiscriminate retention by operators providing electronic communications services of traffic data for a year from the date on which they were recorded for the purpose of combating market abuse offences including insider dealing, is not allowed.

Secondly, the Court addressed the question of whether the French national law should retain its provisional effects. The CJEU argued that leaving aside the state of art with regard to the law in question would result in operators having to comply with obligations relating to the retention of data which, as described above, are contrary to the European law and violate the privacy of a person. Therefore, as a general conclusion, the Court has confirmed that national laws allowing the general and indiscriminate retention of electronic communications data for the purpose of combating criminal offences are not in line with the EU law and cannot be based on the objective of Directive on Market Abuse.

Experts' comments

Iwona Różyk-Rozbicka

This particular case served as another occasion for the CJEU to confirm its strong position in favour of protecting the private lives of users of electronic communications services that was already expressed in a settled case-law of the Court (such as the judgment of 6 October 2020, La Quadrature du Net and Others (C-511/18, C-512/18 and C-520/18), or the judgment of 5 April 2022, Commissioner of An Garda Síochána and Others (C-140/20), as well as in a judgment delivered on the same date in joined Cases C 793/19 and C 794/19. The preliminary ruling of the Court was delivered in the context of French law requiring providers of electronic communications services to retain, for a period of one year, traffic data of all users for the sake of combating market abuse offences. The Court is of the opinion that national legislation requiring, as a preventive measure in the fight against crime, general and indiscriminate retention of traffic or location data belonging to all users of electronic communications services, is precluded in light of Directive 2002/58 (ePrivacy Directive). The issue here is not even the timeframe of retention, but the very fact that it concerns all users, regardless of their possible connection with the investigated crime (in fact, there may not even be a crime committed). Such legislation falls outside of what is strictly necessary and justified in a democratic society, as is required by Article 15(1) of the ePrivacy Directive. We should bear in mind, however, that at the same time the CJEU acknowledges the fact that the directive allows for the general and indiscriminate retention of data for a limited period of time in exceptional cases, such as a serious threat to national state security (the problem how to reconcile these exceptions with fundamental rights was considered at length in La Quadrature du Net judgment).

Vyriausioji tarnybinės etikos komisija

C-184/20

#specialcategoriesofdata

#privacy #article9

7

Background

OT is the director of QP, an entity receiving EU funds and operating in the field of environmental protection. Pursuant to the Lithuanian law, persons working in the public service or in the public interest are obliged to provide a "declaration of public interests" which aims at combatting corruption and documenting potential conflicts of interest. OT failed to provide such a declaration due to the alleged infringement of this data subject's privacy rights stemming from the fact that some of the information to be filled included details concerning their spouses, cohabitants or partners. The required declaration would then be published on a public website. Despite the fact that a lot of sensitive data would not be disclosed, the name of the data subject's partner would remain visible. OT, by refusing to complete a declaration, was then accused of breaching Lithuanian law but challenged that decision on the grounds that the information required in the form could disclose the sexual orientation of this person. Following a national legal action, two question were referred to the CJEU. The first question asked whether Article 6 GDPR should be understood in a way that precludes national law from requiring a disclosure of declarations of private interests and their publication on the controller's website so that all internet users have access to it. The second question concerned the understanding of Article 9 and if it should be interpreted as meaning that that national law may not require the disclosure of data relating to declarations of private interests which may disclose personal data, including data which make it possible to determine a person's political views, trade union membership, sexual orientation and other personal information, and its publication on the website of the controller, providing access to that data to all individuals who have access to the internet.

Judgment

The Court first underlined the fact that data protection and privacy are not absolute rights and that they should be balanced against other competing interests, in that case with transparency, impartiality and the fight against corruption. Thus, the Court went on to perform a balancing of interests consisting of analysis of suitability, necessity and proportionality of the measure. With regards to suitability, the Court decided that it is fulfilled as placing of the filled declarations online ensures transparency and serves the purpose of fighting corruption. Second, when assessing necessity, it was established that while requiring such information may be appropriate, placing it online seems to go beyond what is strictly necessary for the purpose at hand also considering that there is a lack of adequate control over the published data. As regards to proportionality, the Court observed that the measure could be justified by its benefits, namely, the strengthening of the transparency and impartiality of the recipients of public funding. Nevertheless, as the necessity requirement was not met, the Court answered the first question in the affirmative, underlining that what prevailed in its conclusion is the duty to publish the information, rather than any weight of the concerned person's position in the public administration.

As regards the second question, the focus shifted onto the kind of data revealed by the declarations. The Court confirmed that although it was not of a sensitive nature per se, it could potentially reveal information protected by article 9 GDPR. When names of spouses or partners are being shown, it is easy to determine the person's sex and thus, the sexual orientation of the data subject who fills out the form. Therefore, including such personal details in a declaration and publishing it online for all users to see violates the privacy of the person.

Experts' comments

Aleksandra Danielewicz

The decision provides a response to two queries about how to balance other public objectives with the rights to privacy and data protection. First, it shows that privacy rights stand equal amongst other vital interests of an individual and should be protected in various circumstances, even where persons working in a public sphere are involved. The judgment underlines the importance of protecting one's personal information despite their occupation or role within the society and emphasizes how "context" will be the deciding element in finding the proper balance in both cases. However, as the Court emphasizes repeatedly, the factors of fact and law that must be taken into consideration are particular to the matter at hand and are influenced by the legal framework of the Member State in question. Therefore, this finding enables us to state that, in the first issue, the administrative (legal and factual) context of Lithuania influences how privacy, data protection, and openness are balanced. As a result, this finding is not immediately or necessarily relevant to other scenarios within the EU (i.e. other Member States may pursue a more zealous anti-corruption strategy that would tighten transparency controls and - lawfully - limit the rights to privacy and data protection, so long as the "essence" of these rights is not compromised). Similar findings apply to the second question's response as well. The Court takes a contextual approach rather than outlining the exact standards for identifying potentially sensitive personal data. The decision may have significant implications as the CJEU's decision dramatically broadens the area in which Article 9 of the GDPR is applicable. Unless there is a combination of Art. 9 (2) GDPR, any information that could identify a person's racial or ethnic origin, political opinions, religious or philosophical beliefs, political views, trade union membership, health status, or sexual orientation is covered by Art. 9 GDPR. Although the Court intends to provide a high level of privacy and data protection, consistent with prior case law, this approach does not support a uniform interpretation of the law across EU Member States and does not provide legal certainty to data controllers.

Paulina Węgrzynowicz

This judgment is of great importance for two reasons. First, as it stressed the importance of a balancing test and second, as it came to the conclusion that inferred data can also be considered personal data. With regard to the proportionality test, the CJEU stressed that privacy and data protection, although of great importance, are not absolute rights and in case of competing interests, they should be balanced against other legitimate rights and interests. While debating on the balancing test, the CJEU considered placing the data in question online as suitable and proportionate to achieve the purpose of preventing and combating corruption, however, it ruled that other measures less restrictive of the rights to respect for private life and to the protection of personal data of the considered data subjects could be taken to achieve the purpose. Therefore, the necessity requirement was not met. When answering the second question, the CJEU ruled that name-specific data of a data subject's spouse or partner could reveal the data subject's personal orientation if an "intellectual operation involving comparison or deduction" is conducted. While this appears to be sensible, the CJEU did not provide clear criteria for establishing the potentially sensitive personal data.

Proximus

C-129/21

#publicdirectories #consent #telephoneserviceoperators

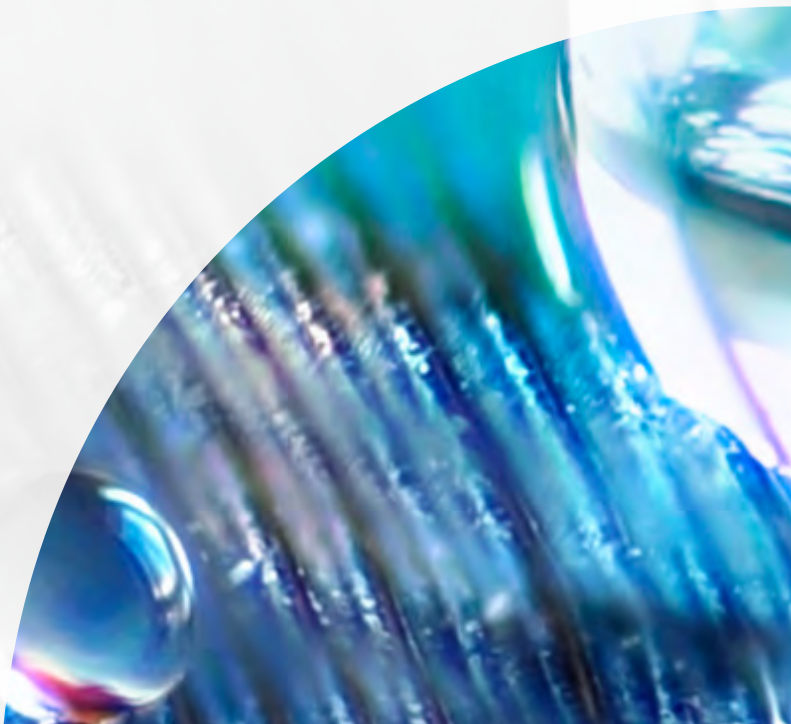
8

Background

Proximus is a provider of telecommunications services in Belgium which also publishes telephone directories and directory inquiry services. Contact details of subscribers are provided to Proximus by operators and only in case where a person has explicitly stated that they do not want to be included in the directories, their data remains left out. Telenet is one of the telephone service operators cooperating with Proximus to which contact details of one of the subscribers were provided. The said subscriber asked for his data not to be included in directories, however, after a subsequent update of this subscriber's contact details, the data was no longer marked as confidential and personal information was shared among the parties concerned and included in the directories. The subscriber lodged a complaint to the Belgian Data Protection Authority which decided in favour of that person and ordered Proximus to comply with the GDPR rules and pay the infringement costs. Proximus did not agree with the decision and appealed before the Belgian Court, arguing that no consent is needed for a publication of data in directories and that they remain under an "opt-out system" which requires a specific request to be excluded. Due to uncertainties surrounding the topic and divergent views on the law, the Court referred a preliminary question to the CJEU.

Judgment

In its decision, the CJEU confirmed that in order to publish the personal data of a subscriber in a public directory and in case of any subsequent processing by third parties for the same purpose, a free, specific, informed and unambiguous consent is needed. It is not necessary that the data subject is aware of the identity of all the providers of directories, but it is important that their wish to be included has been clearly demonstrated. Accordingly, the Court noted that subscribers should also have a possibility to withdraw their consent and make use of the right to be omitted granted by the GDPR. Moreover, the judgment explained that providers such as Proximus are obliged to inform potential other recipients of the subscriber's data about the withdrawal. It is also important to note that operators who have communicated personal details are aware of consent being withdrawn so that the directories can be updated, and data is not forwarded to other parties. Lastly, it was underlined that providers such as Proximus are required under the GDPR to inform search engine providers about an erasure request lodged by the subscriber.



Experts' comments

Paweł Gruszecki

This judgment is interesting for three reasons. Firstly, it concerns the activities of three categories of entrepreneurs: providers of telecommunications services who also publish telephone directories and directory enquiry services, providers of directories, and internet search engine providers. Secondly, the judgment deals with the interplay between the provisions of the GDPR and the sector regulations, i.e. Directive 2002/58. Thirdly, the CJEU found that in circumstances such as those considered in the proceedings, the controller is obligated: (i) under Article 17(2) of the GDPR to ensure taking all reasonable steps (taking into account available technology and cost of implementation) to inform search engine providers of a request made by a personal data subject to erase their personal data; and (ii) under Article 5(2) and 24 of the GDPR to ensure that appropriate technical and organizational measures are applied to inform third-party controllers that the subject of the personal data processed by these controllers has withdrawn consent for processing.

Reading the facts described in this judgment also provides an interesting insight into how the processes in place between the involved entities for communicating that personal data subject is exercising their right under the GDPR should be improved. This is because in this particular case, one of the above entities - despite receiving a request from the personal data subject and marking the new status in the system - restored the previous status after updating the data. The lack of consistency between operational processes therefore contributed to the controller's violation of GDPR regulations. Thus, despite the fact that the ruling concerns a rather specific case from the telecommunications sector (publishing telephone directories and providing directory enquiry services), it is expected that it may provide another argument for businesses processing personal data under the model "controller-to-controller" to regulate in detail what it looks like for them to inform each other about personal data subjects' requests, as well as their relationships with the providers of major search engines. This takes on significance because, according to the ruling, it is sufficient for the data subject to inform only one of many controllers of the withdrawal of consent. In summary, this judgment (insofar as it does not apply only to the telecommunications sector), may be of particular importance, first of all, in cases of brokerage of databases, as well as any other cases of processing of personal data as part of larger value chains (processing personal data under the model "controller-to-controller"), with particular emphasis on those value chains in which there is publication of personal data on the Internet resulting in their indexing by search engines.

Koch Media GmbH v FU

Case C-559/20

#copyright #cappingcosts #nationallaw

9

Background

Koch Media owns intellectual property rights to a computer game called "This War of Mine" on German territory. The game was released in 2014 and gained recognition on the relevant market. Fu, a natural person, committed a violation by publicly sharing the game, without authorization, via a peer-to-peer platform. As a result, Koch Media sent a cease and desisted letter to Fu with a request to stop its unlawful actions and reimburse the incurred legal costs, however, without success. The case was brought before the Court in Saarbrucken, Germany, which accepted the claims presented by Koch Media and judged in favour of the applicant. Despite that, the outcome of the case was not satisfactory for the rights owner as the legal costs awarded to Koch were rather small and constituted only a fraction of what was actually incurred. This is due to the fact that under the relevant provision in German law, the legal costs which can be retrieved are capped if the infringement has been committed by a natural person without a commercial motive. This was later confirmed in a subsequent appeal to a higher instance court. Due to uncertainty as to the compatibility of German law with the Enforcement Directive (Directive 2004/48), including Article 14 under which it should be ensured that reasonable and proportionate legal costs and other expenses should be borne by the infringer, unless equity does not allow this, preliminary questions were referred to the CJEU. The first issue concerned the notion of "other expenses" and whether they include out-of-court legal costs borne prior to filing a lawsuit. The second one focused on the scope of discretionary powers of the national courts with regard to the amounts to be paid for such expenses where the intellectual property rights have been breached by a natural person acting without a commercial interest.

Judgment

Firstly, the CJEU established that the Enforcement Directive applies to extrajudicial, out-of-court proceedings to the same extent as it applies to the costs incurred during the judicial action. The main reason for that is that pre-litigation initiatives, such as the one discussed in the current case, are meant to resolve the dispute outside of courts. Cease and desist letters serve a function of protecting the intellectual property rights of their owner as the very first step which happens before any legal action is ongoing. Nevertheless, it constitutes a valid, legally desirable initiative which could potentially solve the issue and spare the Courts much effort. As such, it is understood that such a cease-and-desist letter, although not falling under the notion of "legal costs", surely can be considered as an "other expense" defined in article 14 of the Enforcement Directive. The Court underlined however that, according to its previous case law, costs which can be captured by that phrase must be directly and closely related to the proceedings at hand.

As regards the second question concerning the cap on costs envisaged in local laws in the case of natural persons acting without a commercial motive, the Court emphasized that possible compensation should be granted for reasonable and proportionate legal costs and expenses incurred. In line with the proportionality principle, the party that won the case should have its costs reimbursed in a significant and appropriate way. Where the capped costs would diminish that effect and result in the right holder being left without proper compensation, the goals of the Enforcement Directive would not be met, and the final outcome would not be fair. Consequently, although the general conclusion was that capped costs are generally capable of serving the need of adequate reimbursement, the European Court ruled that it is possible to deviate from them where the amount of such costs would not be equitable or adequate.

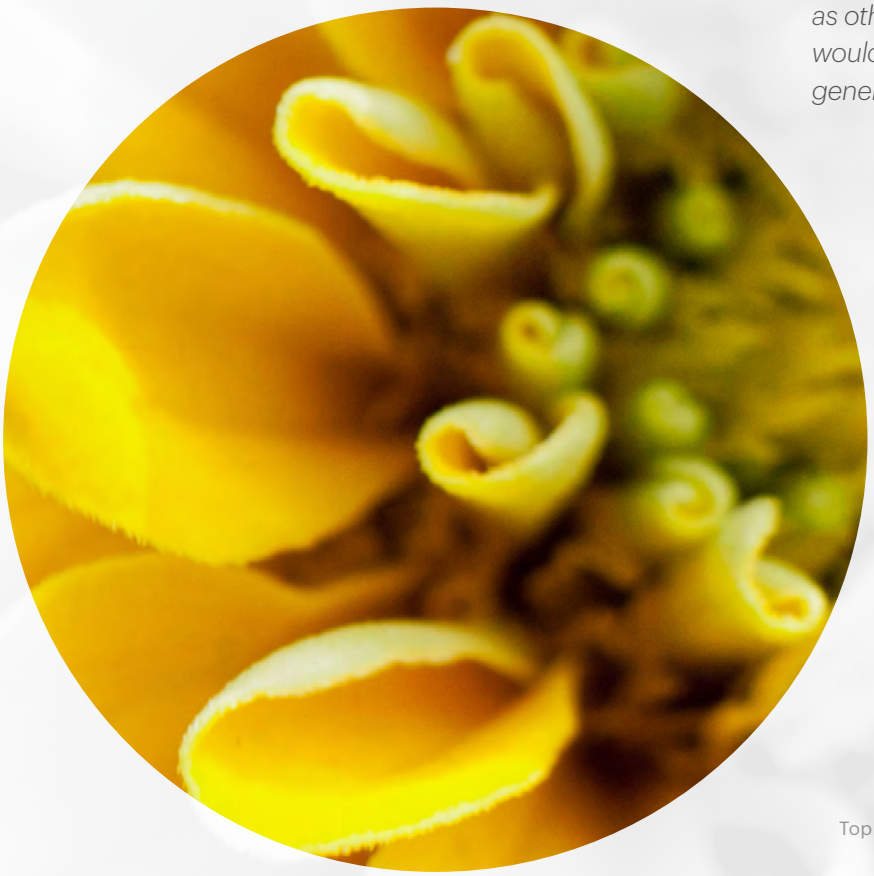
Experts' comments

Barbara Domańska

This ruling largely follows the decision in case C-57/15 (United Video Properties v. Telenet NV) in establishing that out-of-court costs fall within the scope of article 14 of the Enforcement Directive. It should be noted that although the CJEU broadens the scope of "other expenses", it also emphasizes that such costs should remain subject to the review of national judges. In doing so the CJEU strikes a balance between fair and excessive compensation, especially considering how costly out-of-Court proceedings often prove to be.

Marcin Przybysz

The judgement should be positively received by the right holders in the context of retrieving costs of legal services utilised to combat infringements against natural persons prior to filing a lawsuit (e.g. cease-and-desist letters). As the national laws may envisage limitations on such costs when claimed from natural persons who acted without a commercial motive, and also considering that in practice such infringers are often willing to cease the infringement but not really to pay the legal costs, the right holders often have to calculate the cost effectiveness of a possible court action. The actual legal costs borne often extensively exceed such amounts capped in the local laws. In this context the CJEU not only confirmed that such costs of pre-trial legal services can be ordered, but also confirmed that although the limitations of such costs in national laws may be justified in the case of natural persons acting without a commercial motive, such limitations should not result in unjust judgements being issued. Thus, in specific cases the courts may deviate from such limitations and higher amounts can be granted. I believe that it is definitely a justified position, as otherwise a dissuasive effect of court remedies would be diminished, which would contradict the general purpose of the Enforcement Directive.



K K Water

T-610/21

#trademark #similarity #likelihoodofconfusion

10

Background

L'Oreal, the company specializing in the hair treatment industry, sought to register a figurative sign "K K WATER" for goods related to hair care and preparation. Following that, an opposition has been filed by Mr Arne-Patrik Heinze, who based it on an earlier mark "K" which covers similar goods such as shampoos and lotions. The opposition was initially rejected by the EUIPO as no risk of likelihood of confusion was determined. After a subsequent appeal to the Board, the decision was however annulled on the grounds that the relevant public in the EU could perceive the signs as coming from one source due to their name similarity and almost identical goods that they represent. The case then went to the General Court where once again, no likelihood of confusion was established as the contested similarities were deemed insufficient to find that there was such risk. After this conclusion has been reached, no appeal to the CJEU has been noted within the two-month period relevant for initiating any further action. At the time of publishing this report, we were not aware that any such action took place.

Judgment

The court noticed that the risk of confusing two signs cannot be ruled out without at least some consideration as the marks share visual and phonetic elements and are registered for identical goods. The relevant public in the case at hand consist of the same persons as potential hair product buyers who may be confronted with both signs at the same time. Nevertheless, the Court established that the disputed marks have a low degree of visual and phonetic similarity and are conceptually different. According to the CJUEs reasoning, the consumer inspecting the goods would not believe that they come from the same source and are linked with each other. The Court also underlined that distinctiveness of the sign is only a single factor in the overall assessment on the likelihood of confusion and alone does not suffice to establish such risk, especially when taking into account the aforementioned differences and similarities of a low degree. Furthermore, attention was shifted to the styling of the letter K, shared by both of the marks. The Court noticed that having a capitalized letter within a trademark cannot constitute a basis for likelihood of confusion as this could amount to the monopolizing of a single letter for a specific range of goods. To conclude, it was confirmed that the purpose of the opposition proceedings is not to prevent the registration of other marks which also contain that letter but to ensure that the single-lettered sign of high stylistic similarity is not accepted as this would in fact create a risk of confusion.

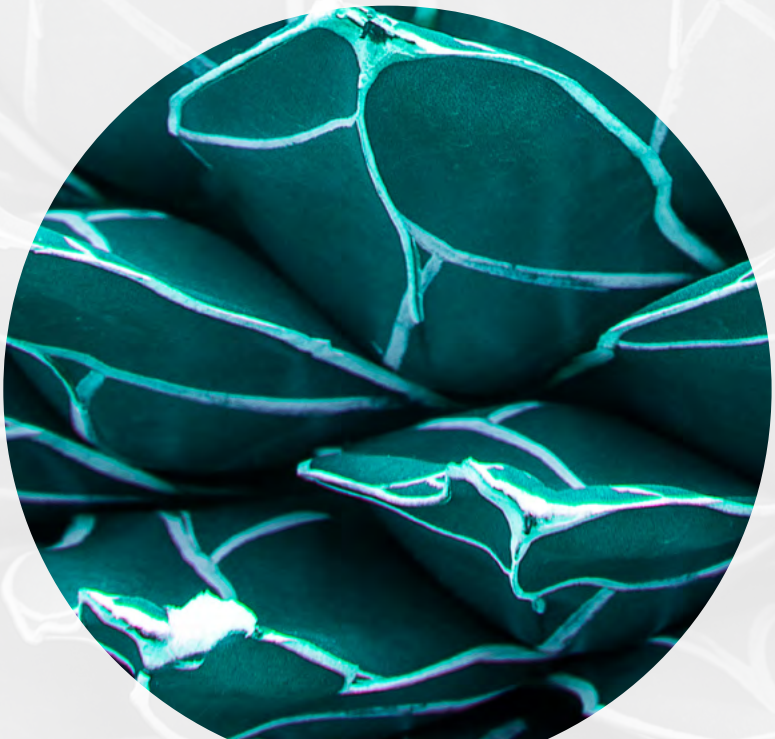
Experts' comments

Marek Trojnarski

The judgment may be surprising to owners of single-letter trademarks. Such marks have been successfully registered and provided their owners protection against similar single-letter trademarks. When comparing word-figurative trademarks, substantial attention is given to identical word elements if they constitute distinctive elements of the brands. Single letters, although practically more difficult to protect, may enjoy protection as registered trademarks if they do not correspond with the characteristics of products covered. Moreover, EUIPO follows in its practice the CJEU judgment of 2011, in which the Court dismissed the argument that single letters are generally per se devoid of distinctive character and that, therefore, only their graphic representation would be protected. The EUIPO applies these criteria both to word and word-figurative marks. The reasoning provided in the ruling may respond to a growing number of registered trademarks and concern for remaining players not having not much manoeuvrability when branding their products. However, it is an accepted practice when examining single-letter trademarks that generic arguments, such as those relating to the availability of signs due to the limited number of letters, should not be followed. The Court has already shared some views in past rulings – which the court relied on in the case at hand - that single-letter trademarks are of weak distinctive character where that letter is not stylised. However, the cases the Court relied on do not apply to identical set-ups as in the case at hand, e.g., the stylization of conflicting marks in one of the past judgments cited by the Court was evidently non-standard. Whereas in the case at hand, I do not believe that the stylization of the marks is distinctive at all. Personally, I do not find the reasoning given in the judgment convincing, especially bearing in mind the very simple and non-distinctive stylization of both marks. The trademark law by definition follows the "first come first served" rule. Other players still have an infinite number of brands they may adapt for their offering. Also, I do not share the view that single-letter trademarks – if not highly stylized – are by definition of weak distinctive character. I believe that customers, accustomed to many forms of trademarks used on the market, as long as a specific letter does not correspond to the characteristic of the goods covered, may view same single-letter trademarks similar and originating from the same business. This applies to one-letter marks stylized differently, assuming the stylization is not far-reaching. The consumers may easily assume that the new stylization of the same-letter trademark was simply a result of rebranding introduced by the trademark owner. The interpretation provided in the ruling, if fully followed, would undoubtedly deprive single-letter trademark owners of protection they expect to enjoy based on their registrations. I believe the owners of existing marks will now need to work much harder on substantiating the oppositions they file to convince examiners that risks for their brands and consumers remain high if same single letter trademarks are used on the market.

Marta Stefanowicz

This judgment develops practical guidance on the likelihood of confusion when short marks are under comparison. It provides a warning that although according to the legislature signs consisting of one letter may constitute an EU trademark, in practice, protecting single letter trademarks against competitors can be a challenging exercise. In the present case, the distinctive character of an earlier single letter trademark, stylized "K", was not disputed. The Court, taking into account the previously established case law, considered that the inherent distinctive character of the earlier mark was normal with regard to the designated goods. When addressing the likelihood of confusion, the Court confirmed that when it comes to the overall assessment of likelihood of confusion, when comparing two marks consisting of an identical single letter, the visual impression has the major role in deciding on the possible confusion. In this context, the Court also reaffirmed that when faced with short signs, the relevant public is likely to perceive the visual differences between them more clearly. Consequently, the likelihood of confusion can be excluded, when two conflicting marks are stylised in a sufficiently different way or contain an additional element that can differentiate the compared marks. In this case, it was found that two marks consisting of the same capital letter, but stylized in a different way, and combined with other word element, are different enough not to cause a risk of confusion. It was highlighted by the Court that a contrary conclusion would mean granting a monopoly over one capital letter of the alphabet for a specific range of goods. The Court pointed out that the purpose of the opposition brought based on a sign consisting of a single letter is to prevent the registration of a trademark which may give rise to a likelihood of confusion with an earlier mark, in particular with regard to its stylistic similarity; and not to prevent the registration of a trademark just because it represents the same capital letter. The basic practical question which arises upon analysis of this judgment, is not whether businesses may register a simple single letter as a trademark, but rather what value does it have when it comes to differentiating a brand among competitors. There are currently over 700 trademarks for a stylised letter K in the EUIPO registry and approximately 60 trademarks consisting of a stylised letter "K" solely in class 3 (covering cosmetics and toiletry products). Unless the use of a single letter trademark is made in a very consistent, long, and notorious way that leads to market recognition and enhanced distinctiveness, policing single letter brand may cause difficulties for mark owners. The essence of a trademark lies in its capacity to differentiate a product from another and enforce the exclusive right against competitors. Choosing a right and valuable trademark is a complex exercise requiring forward thinking and good understanding multi-layered court practice applied to the comparison of trademarks.



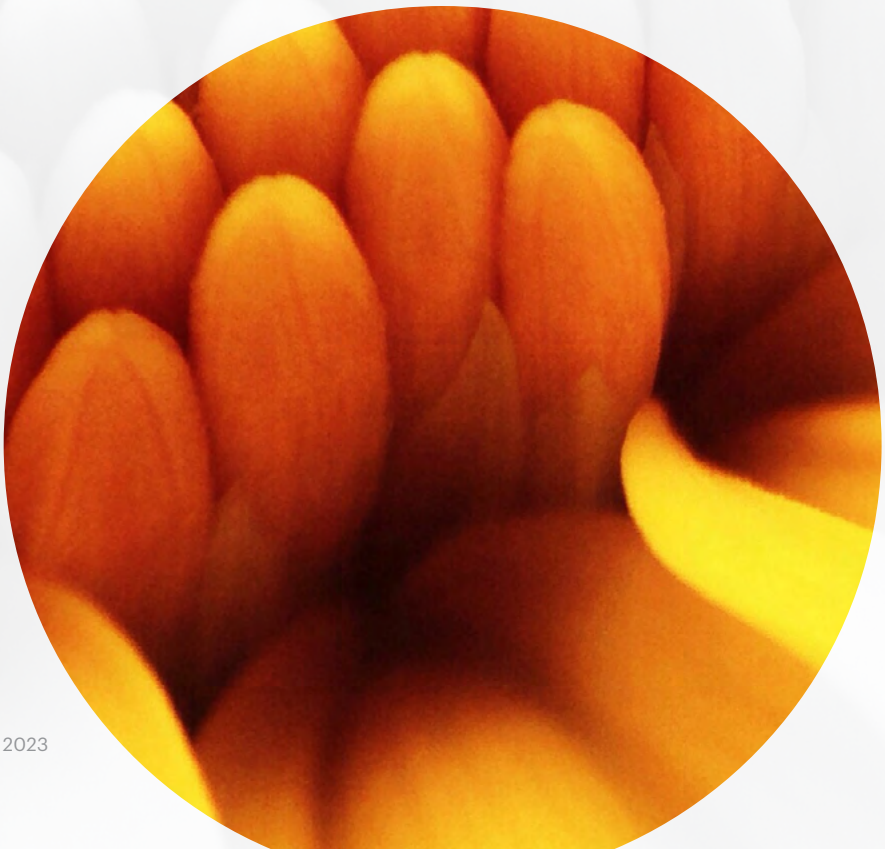
Key upcoming CJEU judgements

Subject matter

Intelectual property

Case reference	Summary	Opinion of the AG (yes/no)
Grand Production (C-423/21)	The case concerns Grand Production d.o.o., a Serbian company producing TV programmes which are broadcasted by a local company GO4YU, managing an online streaming platform. The latter had obtained a license to make the content available, but it was limited to certain territories. Users would circumvent this limitation and access the programmes of Grand Productions via a VPN. Despite the series of interim injunction applications, the case went to an Austrian Court which later referred a preliminary question to the CJEU, asking whether the operator of a streaming platform is liable for copyright infringements when users of the service have used a VPN to access the streamed content that would otherwise not be available in a said territory.	Yes
Česká národní skupina Mezinárodní federace hudebního průmyslu, z. s. v I&Q GROUP, spol. s r.o., Hellspy SE (Case C-470/22)	The case Česká národní skupina Mezinárodní federace hudebního průmyslu, z. s. v I&Q GROUP, spol. s r.o., Hellspy SE concerns three questions referred to the CJEU. The first one relates to the E-Commerce Directive and its liability regime for providers of hosting services and the manner of offering their services. The second question goes a step further and aims at confirming that the private law liability for the said providers cannot be excluded when a chosen business model for running a hosting service could potentially benefit from copyright infringements. Lastly, the CJEU is being asked whether the liability waiver provided in the Directive applies to the provider of an information gathering service if that manner encourages the service recipient to store the information on it without the consent of the copyright holders, but without the active participation of the service provider in the copyright infringement.	No
La Quadrature du Net and others v Premier ministre, Ministère de la Culture (Case C-470/21)	La Quadrature du Net and others v Premier ministre, Ministère de la Culture is a case that emerged in the French Council d'Etat and concerns the retention and access to internet users' data. More specifically, the issue revolves around the general and indiscriminate retention of IP addresses, pointing to their connection source, for a limited period and for the purposes of crime investigation and prosecution. The request for a preliminary ruling is aimed at confirming that the EU law does not preclude national provisions according to which national authorities can access the data which would enable the identification of persons suspected of online copyright infringements.	Yes
Merck Sharp & Dohme (Case C-149/22)	The case concerns the eligibility criteria for Supplementary Protection Certificates - SPCs for "combination products" containing two or more active ingredients. The referral has been made by the Irish Supreme Court where Merck Sharp & Dome's ("MSD") cholesterol-reducing drug has been challenged by another company – Clonmel. MDS obtained an SPC for monotherapy supported by Ezetrol and for a combination therapy of the drug with another product – simvastatin. The first SPC expired at the time when Clonmel produced a competing drug containing two ingredients protected as a combination therapy. After an infringement claim lodged by the MSD, SPC counter-claimed for revocation of the second SPC. The question concerns the notion of product and what can be protected in the file of active medical ingredients.	No

Lännen MCE (Case C-104/22).	The issue in this case concerns two companies, one of which has used a sign on its online advertisement content that was identical to the EU registered trademark of the second company. The question is thus if in such a situation, the country of the second company, the rights of which were infringed, has jurisdiction over the matter and can invoke appropriate proceedings. To establish whether the answer to the above is affirmative, the CJEU has to determine whether the online advertisement, placed by the first company which resides and operates in a different country, can be deemed to be directed at the overall internet-using public, meaning that it is not restricted to a specific territory, specifically if no such territory has been designated by the advertisement itself. This and additional follow-up questions have been referred to the Court of Justice which will now have to assess the territorial scope of the EU law at hand.	No
Castorama Polska Sp. z o.o., „Knor "Sp. z o.o (C-628/21)	The TB and Castorama Polska and Knor case gave rise to a referral before the Court of Justice which concerns the right to information under article 8 of the Enforcement Directive. TB wished to obtain details about an alleged copyright infringement of images to which a copyright has not yet been established. Castorama Polska and Knor, the defendants, perceived the images to be too trivial to be granted protection. The Polish Court was left unsure whether a copyright must first exist to exercise one's right to information under the Enforcement Directive. For the time being, the Attorney General has expressed his opinion stating that the IP right need not be proven to obtain information.	Yes
Natsionalna agentsia za prihodite (C-340/21)	This case concerns the claims for non-material damage suffered by data subjects whose personal data has been affected by the security incident. The questions referred focus mainly on establishing whether "worries, fears and anxieties suffered by the data subject", experienced as a consequence of a cyberattack, are enough to grant compensation, even in situation where no evidence points to the actual misuse of data.	No
UI v Österreichische Post (Case C-300/21)	Data subject claimed to have suffered damage to his reputation, as well as public exposure and confidence loss after extrapolations conducted by Österreichische Post AG which determined potential political affinities. The processing has been carried out without the data subject's explicit consent and sought compensation for the inner discomfort.	Yes



Authors

Dentons Warsaw IP & Tech team

Karol Laskowski
Partner, Europe Co-head of Technology, Media and Telecommunications
D +48 22 242 51 27
karol.laskowski@dentons.com

Małgorzata Domalewska
Senior Counsel
D +48 22 242 51 71
malgorzata.domalewska@dentons.com

Paweł Gruszecki
Counsel
D +48 22 242 56 13
pawel.gruszecki@dentons.com

Aleksandra Politańska-Kunicka
Counsel
D +48 22 242 51 02
aleksandra.politanska-kunicka@dentons.com

Marek Trojnarski
Counsel
D +48 22 242 57 44
marek.trojnarski@dentons.com

Aleksandra Danielewicz
Senior Associate
D +48 22 242 55 23
aleksandra.danielewicz@dentons.com

Bartosz Dobkowski
Senior Associate
D +48 22 242 57 19
bartosz.dobkowski@dentons.com

Marcin Przybysz
Senior Associate
D +48 22 242 57 68
marcin.przybysz@dentons.com

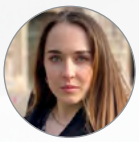
Anna Szczygieł
Senior Associate
D +48 22 242 58 64
anna.szczygiel@dentons.com

Barbara Domańska
Associate
D +48 22 242 58 57
barbara.domanska@dentons.com

Kamil Januszek
Associate
D +48 22 242 52 96
kamil.januszek@dentons.com

Marta Stefanowicz
Associate
D +48 22 242 51 46
marta.stefanowicz@dentons.com

Paulina Węgrzynowicz
Associate
D +48 22 242 52 52
paulina.wegrzynowicz@dentons.com



Anna Kozarów
Paralegal
D +48 22 242 51 90
anna.kozarow@dentons.com

Contributors

Tímea Bana
Partner, Dentons Budapest
Technology, Media and Telecom, Intellectual Property and Data Protection

Zdeněk Kučera
Partner, Dentons Prague
Head of TMT in Prague

We would like to thank Iwona Różyk-Rozbicka for her contribution to this report.

Awards

ABOUT DENTONS

Dentons is designed to be different. As the world's largest global law firm with 21,000 professionals in over 200 locations in more than 80 countries, we can help you grow, protect, operate and finance your business. Our polycentric and purpose-driven approach, together with our commitment to inclusion, diversity, equity and ESG, ensures we challenge the status quo to stay focused on what matters most to you.

www.dentons.com

CSBrand-110774 Top 10 IP&TMT CJEU judgments brochure-03 — 09/03/2023