April 2023

VBB on Belgian Business Law

Issue Highlights

"Van Bael & Bellis' Belgian competition law practice [...] is a well-established force in high-stakes, reputationally-sensitive antitrust investigations."

Legal 500, 2019

Topics covered in this issue

vbb@vbb.com
www.vbb.com

Table of contents

Chaussée de La Hulpe 166
Terhulpsesteenweg
B-1170 Brussels – Belgium

Phone: +32 (0)2 647 73 50
Fax: +32 (0)2 640 64 99

vbb@vbb.com
www.vbb.com

COMPETITION LAW

Belgian Competition Authority Closes Investigation into Roll-Out of Fiber Optic Networks Following Commitments

On 18 April 2022, a prosecutor (*auditeur*) of the Belgian Competition Authority (*Belgische Mededingingsautoriteit / Autorité belge de la Concurrence* – the ***BCA***) announced in a press release the closure of an *ex officio* investigation into possible anti-competitive practices in the roll-out of fiber optic networks in Flanders. This closure follows measures taken by cable operator Telenet and utility company Fluvius to address competition law objections raised against them.

Telenet has a nationwide mobile network and a hybrid fiber coaxial (***HFC***) network in Flanders, parts of Brussels and a few municipalities in Wallonia. Fluvius not only offers various public utility services (including electricity and gas distribution, public lighting and sewage) but also manages an HFC network in Flanders that is owned by four intermunicipal association shareholders. Telenet and Fluvius plan to create a full-function joint venture, NetCo. Following this transaction, Telenet and Fluvius will contribute their fixed electronic communications network infrastructure to NetCo and NetCo will operate and further roll out a mixed HFC and fibre to the premises (***FttP***) network within the current geographic footprint of Telenet and Fluvius.

On 17 June 2022, the BCA launched an ex officio investigation into the rolling out of fiber optic networks in Flanders (*See*, this Newsletter, Volume 2022, No. 6). It now appears that the investigation specifically concerned the setting up of NetCo. Stakeholders reportedly complained that NetCo would give rise to conflicts of interest distorting competition in the deployment of fiber networks, due to (i) Fluvius' indirect ownership by Flemish cities and municipalities responsible for the granting of public works permits; (ii) Fluvius' unique position as a network operator in the fields of energy, heating and water; and (iii) the dealings between Fluvius and telecommunications network operators in the framework of public work synergies.

Telenet and Fluvius responded to these concerns by taking a series of measures that will apply for seven years.

- NetCo will remain autonomous and seek all permits and regulatory approvals required for the deployment of its HFC and/or FttP network independently from Telenet and Fluvius.
- NetCo will bear the costs associated with the deployment of its networks, including its own expenses linked to public work synergies.
- Fluvius will refrain from engaging with cities and municipalities on behalf of NetCo and will explicitly and regularly remind them of the importance of maintaining a level playing field when granting permits for fibre roll-out.
- Measures are taken to generally prevent the exchange of network deployment information between NetCo and Fluvius (with exceptions).
- NetCo and Fluvius commit to complying in good faith and in accordance with applicable competition law principles with the decree governing the exchange of information regarding the use of public domain (*Decreet van 4 april 2014 houdende de uitwisseling van informatie over een inname van het openbaar domein in het Vlaamse Gewest*) and the code governing infrastructure and utilities.
- Fluvius and NetCo will have a central contact point for inquiries, comments, and concerns related to the implementation of existing regulations.
- Fluvius and NetCo will annually report to the BCA.

COMPETITION LAW

While it did not formally approve these measures, the BCA indicated that they "constitute relevant facts" which caused it to end its investigation without deciding on a possible competition law infringement. The BCA stressed that it would open a new investigation "in case of serious indications of possible competition law infringements". It added that it would continue to investigate third party concerns "that are unrelated to the creation of NetCo and thus fall outside of the scope of the present investigation".

Separately, the European Commission authorised the transaction under the EU merger control rules on 30 May 2023. In the press release accompanying its (not yet published) decision, the Commission indicated that it "took note" of the measures taken by Telenet and Fluvius in response to the concerns raised by the BCA (case M.10994).

Chief Prosecutor of Belgian Competition Authority Seeks Interim Measures against Proximus in Edpnet Case

On 20 April 2023, the Chief Prosecutor of the Belgian Competition Authority (*Belgische Mededingingsautoriteit / Autorité belge de la Concurrence* – the ***BCA***) announced that he would request the Competition College (*Mededingingscollege / Collège de la Concurrence*) of his own initiative to impose interim measures on Proximus in an investigation for possible abuse of dominance resulting from the intended acquisition by that firm of edpnet.

This move is unprecedented at several levels.

First, the Chief Prosecutor's request came in response to the acquisition by telecommunications operator Proximus of competing internet provider edpnet. Although this acquisition did not meet the turnover thresholds that would trigger a review under the merger control rules, the BCA nevertheless decided to investigate the transaction under the rules prohibiting the abuse of a dominant position (Article 102 TFEU and Article IV.2 of the Belgian Code of Economic Law). This unusual initiative was taken in the wake of the recent Towercast judgment in which the Court of Justice of the European Union confirmed that Article 102 TFEU may apply to non-notifiable mergers (*See*, this Newsletter, Volume 2023, No. 3).

Second, this is the first time that the Chief Prosecutor seeks interim measures without any request to that effect from a market player or other stakeholder. In a press release available on the website of the BCA, the Chief Prosecutor explained that the aim of the requested measures is "to ensure the continuity of the activities of edpnet", which was in the midst of a judicial reorganisation prior to its acquisition by Proximus. The Chief Prosecutor added that he would maintain "[edpnet's] operational and commercial independence from Proximus pending the outcome of the investigation on the merits". The press release mentions that the Competition College is expected to rule on the request for interim measures in the first half of June 2023.

CONSUMER LAW

European Commission Proposes Right to Repair and Measures against Greenwashing

On 22 March 2023, the European Commission (***Commission***) published two proposed Directives aiming to protect consumers and contribute to the climate and environmental objectives of the European Green Deal: (i) a Proposed Directive on common rules promoting the repair of goods; and (ii) a Proposed Directive on the substantiation and communication of explicit environmental claims ("green" claims).

Proposed Directive on Common Rules Promoting Repair of Goods

Due to the difficulty for consumers to request repairs, consumers tend to discard and replace viable goods that can be repaired. These discarded products result in waste, loss of resources, and a vast amount of greenhouse gas emissions. In addition, replacement is typically more expensive for consumers than repair.

The Right to Repair proposal aims to tackle obstacles that discourage consumers to have their products repaired due to inconvenience, lack of transparency or restricted access to repair services. The proposal thus encourages repair as a more sustainable consumption choice.

The proposal introduces a general right to repair for consumers, both within and outside the statutory guarantee. Within that guarantee, sellers will be required to offer repair, except when repair is more expensive than replacement. Outside the statutory guarantee, consumers will be given the following rights and instruments that will make repair a more accessible choice:

- the right to claim repair from producers for products that should be technically repairable according to EU law (*e.g.*, television sets, vacuum cleaners, and washing machines);
- the duty for producers to inform consumers about the products which they are obliged to repair;
- an online platform that will connect consumers with repairers and sellers of refurbished goods and should enable searches by location and quality standards;
- a European Repair Information Form which consumers may request from any repairer containing information on the repair service offered; and
- a European quality standard for repair services that will help consumers identify repairers who commit to a higher quality level.

More information on the proposal is available here and here.

Proposed Directive on Green Claims

Back in 2020, a Commission study on environmental and green claims found that the majority of these claims were vague, misleading or unfounded, and that nearly half of these claims were unsubstantiated.

The Commission's proposal intends to tackle these "greenwashing" practices by introducing minimum standards for firms to substantiate their green claims and communicate them to consumers. The proposal provides for the following measures:

- prior to making green claims, firms must ensure that the claims form the subject of scientific analysis that identifies the environmental impact of the product, as well as any possible trade-offs;
- the use of aggregate scoring of a product's environmental impact (*i.e.*, scoring based on a combination of elements such as biodiversity, climate, water consumption and soil) will only be permissible if EU rules allow it;

CONSUMER LAW

- any comparison of products or organisations should be made on the basis of equivalent information and data;
- environmental labels should be reliable, transparent, independently verified and regularly reviewed;
- new public labelling schemes may only be developed at the EU level while new private labelling schemes should be subject to pre-approval and show higher environmental ambition than their existing counterparts.

More information on the proposal is available here.

Both proposals will now be reviewed by the European Parliament and the Council of the European Union.

Chamber of Representatives Adopts Bill on Consumer Debt

On 27 April 2023, the Chamber of Representatives adopted a Bill inserting Book XIX "Consumer debts" into the Code of Economic Law (***CEL***) (*Wetsontwerp houdende invoeging van boek XIX "Schulden van de consument" in het Wetboek van Economisch Recht / Projet de loi portant insertion du livre XIX "Dettes du consommateur" dans le Code de droit économique* – the ***Bill***). The Bill became the Law of 4 May 2023 inserting Book XIX "Consumer debts" into the Code of Economic Law (the ***Law***).

A summary of the Law's objectives can be found in the October 2022 edition of this Newsletter (*See*, this Newsletter, Volume 2022, No. 10). The Law applies to all business-to-consumer claims, irrespective of their contractual or non-contractual basis.

The Law addresses two principal subjects:

(i) the payment of debts by consumers to firms; and

(ii) the amicable recovery of consumer debts.

Payment of Debts by Consumers to Firms

A new Article XIX.2 CEL introduces the obligation for firms to send, at their own expense, a payment reminder by means of a formal notice if the debtor does not pay. The payment reminder is subject to specific formal and substantive requirements.

Any contractual penalty clause may only be enforced after the expiry of at least fourteen calendar days (to be increased by an additional three business days when the payment reminder is not sent electronically) and will be capped in accordance with Article XIX.4 CEL.

Amicable Recovery of Consumer Debts

Professionals who conduct activities of amicable recovery of consumer debts will be required to register with the Federal Public Service Economy (*FOD Economie / SPF Économie*). However, this obligation does not apply to attorneys, ministerial officers and judicial representatives (*gerechtelijke mandatarissen / mandataires de justice*) when exercising their profession or mandate (new Article XIX.6 CEL). Any formal notice letter claiming payment of consumer debts must include the elements listed in new Article XIX.7 §2 CEL. The subsequent recovery measures are regulated by new Articles XIX.9 and following CEL.

Subject to limited exceptions, the Law will enter into force on 1 September 2023. The Law will also govern the recovery of consumer debts from agreements concluded prior to its entry into force if the delay in payment or the amicable recovery arises after the Law's entry into force.

DATA PROTECTION

European Data Protection Board Adopts New Guidelines on Notification of Personal Data Breach

On 4 April 2023, the European Data Protection Board (***EDPB***) published a new set of guidelines on personal data breach notifications under the General Data Protection Regulation (***GDPR***). This is the fourth set of guidelines on this subject in the EU. The predecessor of the EDPB, the Article 29 Working Party, adopted the first two sets of guidance in 2014 (pursuant to Directive 2002/58, the e-Privacy Directive) and in early 2018 (under the GDPR). Upon the entry into force of the GDPR on 25 May 2018, the EDPB endorsed the second set and went on to publish additional examples in 2021. The earlier guidelines and the EDPB's examples regarding data breach notification are discussed here and here. All these materials clarify the notification obligations of data controllers in the event of a breach of personal data. The newest set of Guidelines seeks to revise and update the existing guidance on data breach notifications.

Meaning of Personal Data Breach

The GDPR defines a breach of personal data as the "*destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed*" (Article 4(12)). The EDPB clarifies this definition by providing examples such as :

- when a device containing a copy of a controller's customer database was lost or stolen;
- when the only copy of a set of personal data was encrypted by ransomware or was encrypted by the controller with a key no longer in the controller's possession; and
- when a hospital may be forced to cancel surgical operations or puts lives at risk if patients' medical data become temporarily unavailable.

The key factor in determining whether an event is a data breach is the risk to individuals' rights and freedoms, which can result in "*physical, material, or non-material damage*" (Recital 75 of the GDPR). While it is clear that in the above examples a breach occurred, the EDPB also provides examples of security incidents which do not amount to a data breach. For instance, the fact that a media company is unable to send newsletters to its subscribers over a period of time is not likely to pose a risk to the rights and freedoms of individuals.

The EDPB recognises three types of data breaches: the loss of (i) confidentiality; (ii) integrity; and/or (iii) availability of data (the so-called "CIA triad"). It states that while "*determining if there has been a breach of confidentiality or integrity is relatively clear, whether there has been an availability breach may be less obvious*". According to the EDPB, there will be an availability breach "*when there has been an accidental or unauthorised loss of, or destruction of, personal data*", even if the situation is temporary. By contrast, unavailability due to a planned system maintenance is not considered a breach of availability.

Notification to Supervisory Authority

The Guidelines analyse the procedural obligations of data controllers in case of a data breach. The first obligation is to notify a competent data protection authority (***DPA***).

The GDPR requires the data controller to notify the breach to the DPA "*without undue delay*" and, where feasible, no later than "*72 hours after having become aware of it*". The EDPB clarifies that the exact moment when a controller will be considered "aware" of a particular breach depends on the circumstances of the case. When presented with clear evidence of the breach, there is no doubt that the controller can be considered to be "aware" of the breach. This is the case, for instance, if a third party informs the controller that it accidentally received the personal data of one of the controller's customers. Notification is also required if there is a reasonable degree of certainty that an availability breach occurred. The EDPB specifies that

DATA PROTECTION

when the controller is informed of a potential breach, it may undertake a short investigation during which it will not be regarded as "aware" of the breach. However, the inspection should begin as soon as possible and should provide the controller with a reasonable degree of certainty as to whether a breach occurred.

Concerning the type of information to be provided pursuant to Article 33(3) GDPR – such as the nature of a data breach and its likely consequences – the EDPB suggests referring to the various types of individuals whose personal data has been affected by a breach and referring to the different types of personal data that the controller may process (*e.g.*, health data, educational records, social care information, etc.). The EDPB adds that, even if the controller were not to have all the necessary information concerning a breach within 72 hours, it should still inform the DPA which should then decide on how and when additional information is to be provided.

In case of cross-border breaches, the EDPB recommends notifying the lead DPA, which is not necessarily the authority with jurisdiction of the place where the affected data subjects are located or where the breach occurred. The controller should indicate whether the breach involves establishments located in other Member States and should identify the Member States in which data subjects are likely to have been affected by the breach.

However, this does not apply to non-EU controllers that are not established in the EU (Article 3(2)). In accordance with Article 27 GDPR, the non-EU controller should designate a representative in the EU where Article 3(2) GDPR applies. Still, the EDPB explains that the presence of representatives in a Member State does not cause the one-stop-shop system to apply. As a result, the controller has the responsibility to notify the breach to *each supervisory authority* of Member States where data subjects are affected by the breach. This may create particular challenge given the short period of time available for data breach notifications.

Finally, the EDPB specifies that data breaches that are not likely to result in a risk to the rights and freedoms of individuals do not require notification. It cites the example of personal data that are already publicly available.

Communication to Data Subject

The second obligation of a data controller in case of a data breach is to notify the affected data subjects, in addition to the competent or lead DPA, if there is a high risk for the rights and freedoms of the individual.

For instance, this would be the case if a controller stored a backup of an archive of personal data encrypted on a USB key and the key was stolen during a break-in. This also applies to cyber-attacks where individuals' personal data is exfiltrated.

By contrast, a breach of confidentiality involving properly encrypted personal data may not have to be notified to the supervisory authority and to the data subjects when it is unlikely to result in a high risk to individuals. The EDPB provides a list of criteria to consider for assessing such a risk. These are (i) the type of breach; (ii) the nature, sensitivity, and volume of personal data; (iii) the ease of identification of individuals; (iv) the severity of the consequences of the breach for individuals; (v) possible special characteristics of the individual; (vi) possible special characteristics of the data controller; and (vii) the number of affected individuals.

DATA PROTECTION

European Data Protection Board Adopts Harmonised Approach to 101 Data Transfer Complaints of Non-Governmental Authority "None Of Your Business"

On 19 April 2023, the European Data Protection Board (***EDPB***) published its report on the taskforce which it established in September 2020 to analyse the 101 complaints filed by the data protection non-governmental authority *None of Your Business* (***NOYB***) regarding transfers of personal data to the United States. In a judgment of 16 July 2020, the Court of Justice of the European Union (***CJEU***) invalidated the EU-US Privacy Shield, the mechanism which organised the transfer of personal data from the European Union to the United States (Case C-311/18 – *See*, our News Alert on the judgment, which is available here). In the aftermath of that case, NOYB filed 101 complaints with various national supervisory authorities (***SA***) pertaining to the use of "Google Analytics" and "Facebook Business Tools" on websites and the processing of personal data resulting from that usage.

At the outset, the EDPB taskforce noted that, before examining the international transfers section (Chapter V) of the General Data Protection Regulation (***GDPR***), controllers must ensure full compliance with other provisions of applicable data protection rules. For example, the controller must ensure that each processing of personal data has a statutory basis as required by Article 6(1) GDPR.

The taskforce went on to observe that there was no compliance with Chapter V if a given transfer of data had been based on the Privacy Shield after 16 July 2020. It added that the use with retroactive effect of standard contractual clauses (***SCC***) pursuant to Article 46(2)(c) GDPR was also not possible. If SCC were concluded, these had to address the specific deficiencies identified by the CJEU. Encryption by the data importer would not suffice if the data importer had a legal obligation to provide the cryptographic keys to a third-country authority. Similarly, anonymisation, including the anonymisation of IP addresses, was not allowed if it occurred only after the data transfer to the third-country importer. If a processor acted as a data exporter for the controller, the controller was the responsible party under Chapter V and bound by Article 28 GDPR.

The taskforce also identified the principle of accountability as of pivotal importance. Controllers (and providers of tools for processing data) were required to prove that they took every reasonable measure to protect personal data under Articles 5(2) and 24(1) GDPR.

In relation to the 101 complaints, the taskforce determined that website operators who used a specific tool (*e.g.*, for behaviour analysis) had to be regarded as determining the purpose and means of processing under Article 4(7) GDPR, unless the SA decided otherwise. The degree of liability had to be determined on a case-by-case basis, considering both the factual and legal elements of each case, and irrespective of any agreements pursuant to Articles 26 or 28 GDPR.

The taskforce concluded that its creation had enabled the SAs to adopt a common position regarding the NOYB complaints. SAs ordered website operators to comply with the requirements of Chapter V, and if necessary, to cease their transfers. Some decisions were adopted in reliance on the One-Stop-Shop mechanism of Article 60 GDPR, while some website operators stopped their operations before the responsible SA could issue a decision. Further decisions are expected in due time.

While the report underlines that the position of the taskforce is not that of the EDPB, it nonetheless offers important insights for website owners.

The report can be found here.

DATA PROTECTION

European Commission Designates 19 Very Large Online Platforms and Search Engines Pursuant to Digital Services Act

On 25 April 2023, the European Commission designated 17 very large online platforms (***VLOPs***) and two very large online search engines (***VLOSEs***) which will now have four months to bring their activities in compliance with the relevant obligations under the Digital Services Act (***DSA***).

The DSA was adopted in July 2022 and aims to regulate the responsibilities of digital service providers that act as intermediaries in the EU to connect consumers with goods, services and content. The DSA's chief features are as follows:

- Users are empowered to report illegal content easily while the resulting reports are handled diligently.
- Advertisements based on sensitive data of the user (such as ethnic origin, political opinions or sexual orientation) are prohibited.
- Minors are protected by a high level of privacy, security and safety. Profile-based targeted advertising towards minors is banned.
- Risks resulting from the dissemination of illegal content and disinformation online are reduced while safeguarding freedom of expression and information.
- Transparency is increased by the access to publicly available data given to researchers and by the obligation to publish repositories of all the advertisements served on the interface.

The European Commission decided that the following companies qualify as VLOPs or VLOSEs under Article 33 of the DSA:

- **VLOPs:**

- Alibaba AliExpress
- Amazon Store
- Apple AppStore
- Booking.com
- Facebook
- Google Maps
- Google Play
- Google Shopping
- Instagram
- LinkedIn
- Pinterest
- Snapchat
- TikTok
- Twitter
- Wikipedia
- YouTube
- Zalando

- **VLOSEs:**

- Bing
- Google Search

Each of these platforms has at least 45 million monthly active users.

These platforms will also have to report their first annual risk assessment to the European Commission. The platforms will have to identify, analyse and mitigate a wide array of systemic risks ranging from how illegal content and disinformation can be amplified on their services to the impact of these phenomena on the freedom of expression and media.

This marks the first phase of the DSA's application. In a next phase, starting on 17 February 2024, other digital service providers that act as intermediaries connecting consumers with goods, services, and content will also be required to bring their activities in compliance with the DSA (*See*, VBB on Competition Law, Volume 2020, No. 12).

The European Commission's press release on the designation of the VLOPs and VLOSEs is available here.

FOREIGN DIRECT INVESTMENT

Regional Parliaments Approve Belgian Foreign Direct Investment Screening Mechanism

On 9 February 2023, the federal Chamber of Representatives adopted a draft bill approving the cooperation agreement of 30 November 2022 (the ***Agreement***) between the federal government, the regional governments and the communities establishing a foreign direct investment screening mechanism (the ***Mechanism***; *Samenwerkingsakkoord van 30 november 2022 tussen de Federale Staat, het Vlaamse Gewest, het Waals Gewest, het Brussels Hoofdstedelijk Gewest, de Vlaamse Gemeenschap, de Franse Gemeenschap, de Duitstalige Gemeenschap, de Franse Gemeenschapscommissie en de Gemeenschappelijke Gemeenschapscommissie tot het invoeren van een mechanisme voor de screening van buitenlandse directe investeringen / Accord de coopération du 30 novembre 2022 entre l'État fédéral, la Région flamande, la Région wallonne, la Région de BruxellesCapitale, la Communauté flamande, la Communauté française, la Communauté germanophone, la Commission communautaire française et la Commission communautaire commune visant à instaurer un mécanisme de filtrage des investissements directs étrangers*) (*See*, this Newsletter, Volume 2023, No. 1).

The Flemish, Brussels and Walloon regional parliaments have since adopted decrees approving the Agreement on respectively 29 March 2023, 31 March 2023 and 19 April 2023. The Mechanism is expected to enter into force on its envisaged date of entry into force, *i.e.*, 1 July 2023, provided that all acts by the relevant parliaments approving the Agreement are published in the Belgian Official Journal prior to 30 June 2023.

The text of decrees can be found here, here and here.

Separately, the Council of Ministers approved on 21 April 2023 rules governing the use of languages for notifying direct investment and in review procedures.

INSOLVENCY

Temporary Measures Expanding Possibilities of Insolvency Are Prolonged Once More

On 31 March 2023, the Royal Decree of 20 March 2023 prolonging Articles 2 and 4 to 12 of the Law of 21 March 2021 modifying Book XX of the Code of Economic Law and the Income Tax Code 1992 (the ***Law***) was published (*Koninklijk Besluit van 20 maart 2023 tot verlenging van artikelen 2, 4 tot 12 van de wet van 21 maart 2021 tot wijziging van boek XX van het Wetboek van Economisch Recht en het Wetboek van de inkomstenbelastingen 1992 / Arrêté royal du 20 mars 2023 portant prolongation des articles 2, 4 à 12 de la loi du 21 mars 2021 modifiant le livre XX du Code de droit économique et le Code des impôts sur les revenus 1992*) (the ***Royal Decree***). As a consequence, the temporary measures on insolvency provided for by the Law will continue to apply until 30 September 2023. These measures created a pre-packaged insolvency procedure and enhanced accessibility to the judicial reorganisation procedure (*See*, this Newsletter, Volume 2021, No. 3).

This prolongation must be viewed against the backdrop of the much anticipated transposition of Directive 2019/1023 of the European Parliament and of the Council of 20 June 2019 on preventive restructuring frameworks, on discharge of debt and disqualifications, and on measures to increase the efficiency of procedures concerning restructuring, insolvency and discharge of debt, and amending Directive (EU) 2017/1132, whose transposing draft bill was finally submitted to the federal Chamber of Representatives on 20 March 2023 and adopted on 25 May 2023. The law will enter into force on 30 September 2023 and will make a further extension of the temporary measures superfluous.

The Royal Decree is available here. The Directive can be found here.

INTELLECTUAL PROPERTY

Court of Justice of European Union Holds That Broadcasting Protected Music on Plane Constitutes "Communication to Public"

On 20 April 2023, the Court of Justice of the European Union (***CJEU***) delivered its judgment in joined cases *Blue Air Aviation Ltd and Societatea Naţională de Transport Feroviar de Călători (SNTFC) 'CFR Călători'* (C-775/21 and C-826/21). It held that the use of copyrighted music for ambient purposes in commercial transport constitutes a "communication to the public" within the meaning of Article 3(1) of Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society (the ***InfoSoc Directive***).

Background and Procedure

Two collective management organisations brought an action against Blue Air Aviation SA (***Blue Air***) for the payment of royalties allegedly due on the offering of background musical works on board passenger aircraft, and against CFR Călători' SA (***CFR***) for the payment of royalties allegedly due on the use of facilities for communicating music on board trains.

The separate actions were brought before the Tribunalul București, Romania (the ***Referring Court***) which referred questions to the CJEU for a preliminary ruling.

CJEU's Reasoning

Firstly, the Referring Court asked whether Article 3(1) of the InfoSoc Directive must be interpreted as meaning that the broadcasting of a musical work as background music in a transportation vehicle constitutes a communication to the public. The CJEU observed that the concept of "communication to the public" must be construed broadly to ensure that a high level of protection is afforded to authors of copyrighted works and to guarantee that these authors receive suitable remuneration.

Citing previous case law, the CJEU repeated the two cumulative criteria necessary for an act to constitute a "communication to the public", *i.e.*, (i) an act of communication of a work; and (ii) the communication of that work to the public.

As regards the question of the Referring Court whether the profit-making nature of a communication is decisive for making this assessment, the CJEU stated that, while it is not irrelevant, the mere fact of profiting from the use of copyrighted material does not, of itself, point to the existence of a communication. It is sufficient that the transport operators, in full knowledge of the consequences of their conduct, take steps to give their customers access to music, while, absent such steps, those customers would not otherwise be capable of accessing it.

On the concept of "the public", the CJEU, in citing its judgments of *YouTube* and *Cyando* (C-6682/18) and *Reha Training* (C-117/15), repeated that the definition of this notion extends to an indeterminate number of potential recipients and therefore implies a "fairly large number" of persons. In this regard, the number of persons travelling on both the Blue Air airplanes and the CFR trains could not be disregarded as insignificant. In addition, the CJEU emphasised that, in order to determine that number, account must be taken of the number of persons who may have access to the same work at the same time, but also of how many of them may access it in succession.

The CJEU concluded that the relevant acts in the cases at hand constitute a "communication to the public", in particular because the copyright-protected work had been broadcast in half of the aircraft operated by Blue Air during flights operated by that airline. As a result, the public in question consisted of all the passenger groups who, simultaneously or successively, took those flights.

INTELLECTUAL PROPERTY

Secondly, the Referring Court asked whether the installation on board of sound equipment and possibly software enabling the broadcasting of background music, constitutes a sufficient basis for making a rebuttable presumption of communication to the public. The CJEU held that Article 3(1) of the InfoSoc Directive guarantees authors the exclusive right to prohibit any communication of their work to the public. Nonetheless, as pointed out by the CJEU in *YouTube* and *Cyando*, recital 27 of the InfoSoc Directive indicates that the mere provision of facilities for public communication does not of itself amount to a communication, since it is merely "a provision of physical facilities intended to enable or carry out a communication". This distinguishes it from acts by which service providers deliberately and knowingly communicate with the public.

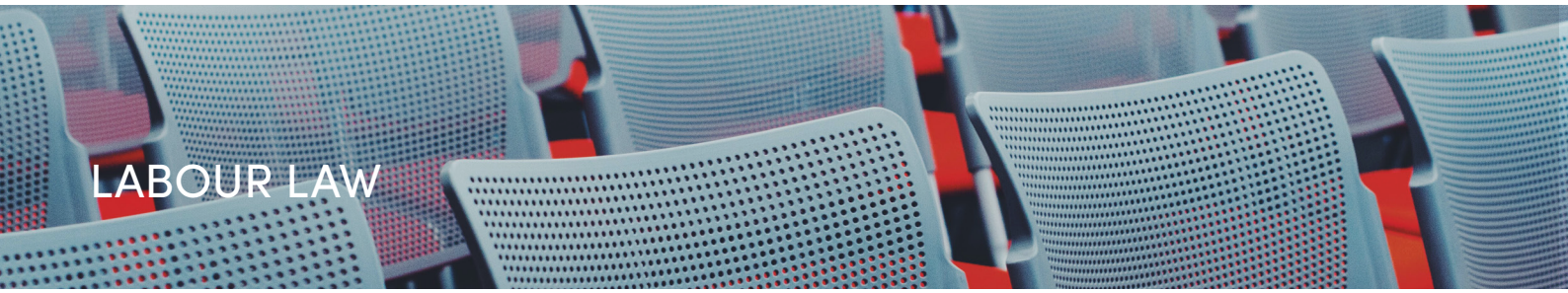
In this regard, the CJEU pointed out that it has already ruled that the operators of a public house, a hotel or a spa establishment perform an act of communication when they deliberately transmit protected works to their customers, by intentionally distributing a signal by means of television or radio sets which they have installed in their establishment. It concluded that the mere installation of sound equipment in a means of transport cannot be comparable to acts by which service providers intentionally transmit protected works to their customers by distributing a signal by means of receivers which they have installed in their establishment, allowing access to such works.

Lastly, in the light of the preceding analysis, the CJEU also held that the fact that the mere provision of physical facilities for enabling or making a communication does not in itself amount to communication precludes national legislation which establishes a rebuttable presumption that there is a communication to the public because of the presence of such sound systems.

Comment

This case represents a continuation of the stream of jurisprudence which defined the concept of "communication to the public". After hotel rooms, spas, rehabilitation centres, dentist's waiting rooms and rental cars, the CJEU has now also held that broadcasts of copyright protected works in airplanes and trains constitute communications to the public. At the same time, it also held that the mere installation of equipment for such broadcasts does not constitute an act of communication to the public.

The judgment can be found here in Dutch, English and French.



LABOUR LAW

National Social Security Office Will Participate in Social Security Framework Agreement on EU Cross-Border Telework

The National Social Security Office (*Rijksdienst voor Sociale Zekerheid / Office National de Sécurité Sociale* – the ***NSSO***) recently announced that it will participate in the Social Security Framework Agreement on EU cross-border telework.

On 29 March 2023, the Administrative Committee for the Coordination of Social Security Systems (the ***Administrative Committee***) reached a consensus on a preliminary framework agreement to establish the applicable social security legislation for cross-border teleworkers within the European Union (the ***Framework Agreement***). The Framework Agreement allows employers and employees to maintain social security coverage in the country of the employer when an employee works from home in another country less than 50 percent of the time.

During the COVID-19 pandemic, a principle of neutralisation was implemented to address the social security position of cross-border workers. Specifically, teleworking days were not considered on a temporary basis when determining the applicable social security scheme to avoid any changes that may arise. Absent such neutralisation, a change in the social security scheme would occur if a cross-border worker were to work over 25% of his or her working time in his/her country of residence, following mandatory homeworking measures imposed to limit the spread of the virus. In the aftermath of the COVID-19 pandemic, workers generally continued to seek greater flexibility in their work arrangements. As a result, in June 2022, the Administrative Committee put forward a recommendation to establish a transitional period for ascertaining the relevant social security scheme for cross-border teleworkers. This transitional phase is scheduled to end after 30 June 2023.

The Framework Agreement is centered around Article 16 of Regulation No. 883/2004 on the coordination of social security systems (the ***Regulation***), which allows for a derogation from the normal principles regarding the applicable social security regime in the event of cross-border work. Normally, an employee who resides in a country different from his employer's location may work up to 25% of his time in his country of residence while still being covered by the social security regime of the Member State of the employer. The Framework Agreement now offers a choice to employers and employees to enable an employee to work for up to 50 percent of his time in his country of residence while still retaining coverage under the social security system of the employer's Member State.

If the employee and the employer agree on applying the Framework Agreement, they should file a request with the social security administration of the employer's registered seat. Provided that approval is granted by the authorities, an A1-certificate will be delivered with a maximum duration of three years, with extensions possible upon request.

LITIGATION

Treaty Relations to Be Established Between European Union and Ukraine on Mutual Recognition and Enforcement of Judicial Decisions

On 24 April 2023, the Council of the European Union (the ***Council***) agreed to establish treaty relations between the European Union (the ***EU***) and Ukraine within the framework of the Convention on the Recognition and Enforcement of Foreign Judgments in Civil or Commercial Matters (the ***Convention***) (the ***Decision***).

The Convention, which was concluded on 2 July 2019, aims to enhance judicial cooperation and commits Contracting States to recognising and enforcing judgments handed down in civil or commercial matters in other Contracting States.

The Convention, which was accessed to by the EU (*See*, this Newsletter, Volume 2022, No. 7) and ratified by Ukraine on 29 August 2022, will enter into force on 1 September 2023. At present, only the EU, its Member States and Ukraine are parties to the Convention.

The Decision clears the path for the EU to enter into treaty relations with Ukraine under the Convention. The Council found that "*there* [were] *no fundamental obstacles, such as related to the independence and efficiency of the judiciary, the fight against corruption or the respect of fundamental rights, which could prevent the EU from entering into treaty relations with Ukraine*". According to the Council, the Decision will facilitate the recognition and enforcement of the EU's and Ukrainian judgments in civil and commercial matters, thereby facilitating international trade and reinforcing ties between the EU and Ukraine.

The Council's press release is available here and the Convention is available here.

Brussels
Glaverbel Building
Chaussée de La Hulpe 166
Terhulpsesteenweg
B-1170 Brussels
Belgium

Phone:+32 (0)2 647 73 50
Fax:+32 (0)2 640 64 99

Geneva
26, Bd des Philosophes
CH-1205 Geneva
Switzerland

Phone:+41 (0)22 320 90 20
Fax:+41 (0)22 320 94 20

London
Holborn Gate
330 High Holborn
London
WC1V 7QH
United Kingdom

Phone: +44 (0)20 7406 1471

VAN BAEL & BELLIS

www.vbb.com