LIGUE INTERNATIONALE DU DROIT DE LA CONCURRENCE
INTERNATIONAL LEAGUE OF COMPETITION LAW
INTERNATIONALE LIGA FÜR WETTBEWERBSRECHT

LIDC BRUSSELS 2021

QUESTION B: Influencers, native advertising and the use of AI for marketing – how can it be controlled by law?

International Rapporteur: Marta DELGADO ECHEVARRÍA (mdelgado@jonesday.com)

HUNGARY
National Rapporteur: Adam, LIBER (adam.liber@liber.hu)

Members of the Working Group: Lili, ALBERT (lili.albert@cerhahempel.hu), Judit, FIRNIKSZ (judit.firniksz@pwc.com), Adam, LIBER

References and abbreviations:

AI	Artificial Intelligence
Competition Act	Act LVII of 1996 on the Prohibition of Unfair and Restrictive Market Practices
Consent Guidelines	Guidelines 05/2020 on consent under Regulation 2016/679
DCT(s)	Digital Comparison Tool
DPbDD Guidelines	Guidelines 4/2019 on Article 25 Data Protection by Design and by Default
DPbDD	Data Protection by Design and by Default
ePrivacy Directive	Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector
draft ePrivacy Regulation	Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC
GDPR	European Parliament and Council Regulation 2016/679 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC, OJ 2016 L 119, p. 1
HCA	Hungarian Competition Authority (*Gazdasági Versenyhivatal*)
Hungarian DPA	Hungarian Data Protection and Freedom of Information Authority (Nemzeti Adatvédelmi és Információszabadság Hatóság)
UCP Act	Act XLVII of 2008 on the Prohibition of Unfair Business-to-Consumer Commercial Practices

1. INTRODUCTION

The emergence of data driven-business models, data analytics and algorithms provide unprecedented opportunities to gain and maintain competitive advantage by big tech service providers whose main income is from analysis, processing and selling of data. However, this also triggers high exposure of individuals through technology because there seems to be significant imbalance between providers and users. The use of digital services and the utilization of algorithms and artificial intelligence is now essential in the enforcement activities of various regulatory agencies, prosecuting consumer protection, competition and data protection infringements and it seems that it is necessary to provide a coordinated answer to the issues raised by new business models considering the interplay between privacy law, competition and consumer protection law issues.

This country report will explore the main aspects of this interplay under EU and Hungarian law.

2. PRIVACY IMPLICATIONS

Regarding the use of algorithms or other AI based applications, chatbots, customer tracking and similar means, the implementation of such technologies inevitable involve the processing of personal data and therefore trigger various obligations under the GDPR. These obligations include securing an appropriate legal basis and transparency; accuracy (data quality); data security; compliance with purpose limitation, data minimization, storage limitation; documentation requirements and the requirement to conduct data protection impact assessments as part of these efforts with a view to the high risks that the use of such technologies may cause to the data subject.

In this context, data protection by design and by default ("DPbDD") is of particular importance when designing applications or algorithms, because the data controller must assess DPbDD requirements which covers the effective implementation of data protection principles under Article 5 (1) GDPR and data subjects' rights and freedoms by design and by default that controllers must take into account when designing the processing. The Hungarian DPA has not yet released any guidance on application design issues; however, the EDPB has released the Guidelines 4/2019 on Article 25 Data Protection by Design and by Default ("DPbDD Guidelines"). The addressee of DPbDD obligations are data controllers. However, controllers (especially small data controllers) have seldom the opportunity to build and design their own systems and the GDPR does not seem to address software developers and manufacturers who play a key role in DPbDD implementation.

This part of the country report explores the privacy implications with reference to the applicable data protection principles under Article 5 (1) GDPR and related accountability obligations under Article 5(2) GDPR.

2.1 Lawfulness and purpose limitation

Under the GDPR, the lawfulness principle requires that the controller must identify a valid legal basis for the processing of personal data. Moreover, to comply with the purpose limitation principle, the controller must collect data for specified, explicit, and legitimate purposes, and not further process the data in a manner that is incompatible with the purposes for which they were collected. To comply with these requirements, the EDPB in its DPbDD Guidelines expects that the whole processing lifecycle must be in line with the relevant legal grounds of processing and that the design of the processing should therefore be shaped by what is necessary to achieve these legitimate purposes.

To the extent *consent* is used to legitimize data processing (Art. 6 (1)(a) GDPR), the goal would be to enable the data subjects (consumers) to make informed decisions, so they could understand what they are agreeing to when providing their personal data, which protects the consumer. According to the Hungarian Advertising Act "*advertisements may be conveyed to natural persons by way of direct contact (…), only upon the express prior consent of the person to whom the advertisement is addressed. The statement of consent may be made out in any way or form, on condition that it contains the name of the person providing it, (…), furthermore, any other personal data authorized for processing by the person providing the statement, including an indication that it was given freely and in possession of the necessary legal information*."

If the data controller relies on *contractual legal bass*, then the controller must check pre-determine what personal data is objectively necessary for the performance of a contract with a data subject or necessary to take steps at the request of the data subject prior to entering a contract. In this context, Article 6(1)(b) GDPR may cover the preliminary processing of personal data being necessary before entering into a contract in order to facilitate the actual entering into that contract by the data subject, such as processing of the data subject's personal data for the purpose of responding to an enquiry; however, it may not cover processing which is carried out solely on the initiative of the data controller, such as service improvement, fraud prevention or behavioural advertising, because these processing operations will require reliance on other legal bases. Article 6(1)(b) GDPR can also cover processing operations objectively necessary for the performance of the contract and deliver of the contractual services, i.e. processing reasonably foreseen and necessary within a normal contractual relationship, such as payment processing, sending formal reminders about outstanding payments or correcting errors or delays in the performance of the contract, contractual warranty, or contract termination and returning

of goods. The processing options, by default, may not allow retrieval of data directly from other sources than the data subject itself, because this will also require a different legal basis. However, the processing of special categories of data could not be covered by solely relying on Article 6(1)(b) GDPR.

The use of advertising tracking cookies can only be legitimized based on consent (pursuant to Section 13/A (4) of the Act CVIII of 2001 on certain issues of electronic commerce services and information society services), whereas consent may not be combined with other legal bases such as legitimate interests (see item 123 of Guidelines 05/2020 on consent under Regulation 2016/679 and item 40 of Opinion 5/2019 on the interplay between the ePrivacy Directive[1] and the GDPR). This is because article 5 (3) of the ePrivacy Directive takes precedence over the legal bases in Article 6 of the GDPR. The GDPR mentions cookies only once, in recital 30. If the cookies are used to identify users, then they qualify as personal data so they are subject to the GDPR. Under the GDPR controllers have the right to process their users' data (the cookies) as long as they receive consent, or if they have a legitimate interest.

Legality of processing may be challenged if the data controller relies on the use of cookie walls, i.e. when consumers may not use a website without consenting to the use of personal data or cookies also likely violate the tie-in ban under Art. 7 (4) GDPR. Under Art. 7 (4) GDPR says "*when assessing whether consent is freely given, utmost account shall be taken of whether, inter alia, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract.*" This provision makes a distinction between processing activities necessary for the performance of a contract, and clauses making the service conditional on certain processing activities that are not in fact necessary for the performance of the contract. If consent is given in this situation, it is presumed to be not freely given. The legal basis of consent and contract cannot be merged and blurred.[2] In practice, Hungarian data controllers seldomly respect the tie ban under Art. 7 (4) GDPR, therefore data subjects erroneously get the impression that they are giving their consent in line with Article 6 (1) (a) when signing a contract or accepting terms of service. This may occur when data controllers request data subjects to "accept" a privacy notice. When consumers are precluded from using a website without consenting to the use of their personal data, the recently updated consent guidelines of the EDPB also provided clarification saying that "*In order for consent to be freely given, access to services and functionalities must not be made conditional on the consent of a user to the storing of information, or gaining of access to information already stored, in the terminal equipment of a user (so called cookie walls)*". Practically, if there is no possibility to access the website content without accepting the cookies and the data subject is not presented with a genuine choice, this will not constitute valid consent and this practice will be illegal.

Under the GDPR, processing must be limited to what the legal basis strictly gives grounds for. Under the GDPR opening clauses, there may also restrictions under member state law that algorithm operators must consider when creating user profiles. Under Hungarian law, the relevant limitations are laid down by the Act XLVII of 1997 on Processing and Protection of Medical and Other Related Personal Data which limits the processing purposes of data concerning health and requires explicit consent of the data subject if the processing purpose does not comply with the Act. Moreover, the Act No XXI of 2008 on the protection of human genetic data and the regulation of human genetic studies, research and biobanks limits the export of genetic data form third countries which do not secure the adequate level of protection for personal data.

2.2 Transparency

Anyone who spends a lot of time on the Internet can hardly afford to read the numerous data protection regulations that apply to advertising, prices, etc. and in practice, data protection declarations are often extensive and difficult to understand.

According to the GDPR's transparency principle, the controller must be clear and open with the data subject from the start about how they will collect, use and share personal data. In this context, the controller must act transparently and present information about the processing in such a manner that makes it easy for data subjects

[1] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), OJ 2002 L 201, p. 37.
[2] Guidelines 05/2020 on consent under Regulation 2016/679, Version 1.1, adopted on 4 May 2020, item 26.

to understand what processing is contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the personal data and of the possible consequences of failure to provide such data.

If the website operator does not know what data is collected from third parties on his website, it is likely that the operator will be unable to comply with transparency requirements under the GDPR.

On 17 February 2017, the Hungarian DPA released cookie guidance relating to website and online shop operations. This guidance says that before implementing cookies or similar technologies placing information on the users' end device, the website operator must (i) map the cookies that it wishes to use on its site and (ii) determine whether notice or consent is required for the use of each. The guidance also confirms that the website operator is liable for the use of third-party cookies which transmit information - such as user behaviour data - to third parties. Accordingly, the website operator must have the user's consent to allow the use of cookies collecting and transmitting user information to third parties. The guidance says that special attention must be given to the use of social plug-in modules monitoring user behaviour or tracking other user activities. The website operator must be aware of the scope of the data collected by third party cookies, including the data categories collected and the relevant processing purposes, such as analytics, advertising or market research. The operator also must be transparent about data collection practices relative to use of its website.

Due to the inherent complexity of the black box operation of modern computing systems, data subject (or even experts) likely will be unable to understand how artificial intelligence made its predictions. However, even if a passenger may be unable to explain the technical operation of the tram or airplane, there is no reason to exclude someone from using these means of travel, because only the travel destination and its safety will be of utmost importance for a passenger.

Algorithmic transparency is a principle expecting that the factors that influence the decisions made by algorithms should be visible, or transparent, to the people who use, regulate, and are affected by systems that employ those algorithms. The EU regulatory model of transparency (Article 12 GDPR) focuses on "meaningful transparency", which means that in case of automated decision-making, including profiling the data controller must provide meaningful information that the average data subject is able to understand at least "*about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject*" (Article 13 (2)(f) GDPR). This also means that information of technical nature that data subjects are unable to understand must be omitted from the disclosure. Within the context of AI operations, transparency should cover information how the algorithm was taught, how its vulnerabilities were addressed, what the data source is; how its results have been validated and what impact it may have on the individual. When being transparent about AI, the data controller must disclose the risks and possible outcomes of the decision-making process, rather than its technical functionality because the latter will be of little value for individuals. Understanding what data is used by the algorithm to determine an outcome can be useful in securing algorithmic transparency. However, because non personal data (such as statistical data) might also play an important role in the decision, the specific amount of personal data used may not be always informative regarding the opacity of the algorithm's operation.[3]

2.3 Accuracy / data quality

According to the accuracy principle, personal data shall be accurate and kept up to date, and every reasonable step must be taken to ensure that personal data that is inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay. Accuracy is of utmost importance because decisions about personalised advertising / content / prices are made by algorithms based on the customer's existing data sets. In order to comply with the GDPR, the advertiser must secure that the quality of the underlying data sets are ensured for the creation of personalised advertising / content / prices.

Data quality means that personal data shall be accurate, relevant, complete, up to date and consistent to comply with the GDPR applicable requirements. Data accuracy principle is one of the kay data protection principles under the GDPR. Article 5 (1) (c) GDPR also requires that personal data is adequate and relevant in relation to the

[3] https://www.europarl.europa.eu/RegData/etudes/STUD/2019/624262/EPRS_STU(2019)624262_EN.pdf item 3.6.2

purposes for which they will be processed. Under the accountability principle (Article 5 (2) GDPR) the data controller must be able to demonstrate compliance with these requirements. The main data quality issues may be incompleteness, inaccuracy (wrong field entered), inconsistency, invalidity, redundancy and non-standard data.

The data management by artificial intelligence can also be improved to use the large amounts of data sensibly and to enable an extended application in real time by employing real time data analytics, which is made available by AI which may provide improved response times and can make the data management process more robust. This technology requires improved processing power and extensive infrastructure, provide increased degree of accuracy and efficiency for data processing and are readily available, state-of-art technologies on the market.

The Hungarian DPA has not released any guidance on the handling of data quality issues. However, the EDPB has released its DPbDD Guidelines which covers compliance requirements regarding data accuracy.

In practice, to secure data quality, the controller may implement tools providing for entry field validations, misspelling detection and handling; email (such as disposable e-mail) and IP blacklist filtering; data cleansing and testing by using static analysis tool, which checks the data against quality issues, such as random white spaces (such as unwanted characters removal); adding predefined choices required input fields, drop-down lists, rather than free text entry possibilities; measurement and introducing metrics regarding data quality and providing the possibility for data subjects to correct the data.

2.4 Fairness

The "fairness" principle requires that personal data shall not be processed in a way that is detrimental, discriminatory, unexpected or misleading to the data subject. In that regard, the ethical aspects of data processing are of utmost importance. In that regard, there are strong arguments[4] that developers and implementers of AI have a social responsibility to incorporate socially and ethically recognised values into the programming design process to avoid unfairness and discrimination that the functioning of the algorithm may cause. As the part of this process developers and implementers must secure the diagnosis and correction of any biases that the algorithm may cause.

It is likely that advertising campaigns, also in the creative field, be able to be carried out autonomously by artificial intelligence in the future. Algorithms evaluate previous purchase decisions and then place new advertisements. This may constitute a discrimination against other companies, which were not subject to previous purchase decisions, because if the data used for the training of the algorithm is selected in a discriminatory way, then the machine learning algorithm will also likely continue the discriminatory practice. The HCA and the Hungarian DPA has no practice in that regard. However, depending on the specific circumstances of the case, this may constitute an abuse with a dominant position *via-á-vis* companies, which were not subject to previous purchase decisions; moreover, data subjects who are exposed to discriminatory data processing, may claim that the data controller did not comply with the fairness principle when processing personal data in a discriminatory way.

The creation of personalised advertising or personalised prices may fall under Art. 22 (1) GDPR provided that data processing activities have serious consequences for individuals. According to the EDPB Guidelines on automated individual decision-making and profiling for the purposes of Regulation 2016/679, only serious impactful effects will be covered by Article 22. According to the GDPR "*profiling means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements*". There are potentially three ways in which profiling may be used, namely (i) general profiling; (ii) decision-making based on profiling; and (iii) solely automated decision-making, including profiling, which produces legal effects or similarly significantly affects the data subject." [5] When the decision is based only on an algorithm, we can

[4] The Institute of Electrical and Electronics Engineers (IEEE) - 'Ethically Aligned Design' First Edition (March 2019)
[5] Article 29 Data Protection Working Party Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, available at https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053. As last Revised and Adopted on 6 February 2018; Last visited on 19 September 2020.

speak about the process described in point (iii). This is what happens exactly in case of personalised advertising and personalised prices that is an algorithm assess the personal data and decides on the basis of the assessed personal data (for example location data or an online identifier).

The creation of personalised advertising or personalised prices may qualify as automated individual decision-making. According to the GDPR, the data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her. It is not explicitly required by Hungarian law that the consumer shall be given a choice between personalised advertisements / prices and non-personalised ones, however it can be derived from the fairness principle of the GDPR.

2.5 Integrity and confidentiality

Data security principle means that controllers and processors must implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk of data processing. To comply with data security requirements, the controller is expected to perform a risk analysis, which assess the risks against the security of personal data and counter identified risks, such as accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed, which may in particular lead to physical, material or non-material damage.

Considering the privacy risks that the use of artificial intelligence may pose for the individual, such operations will likely trigger the requirement of a data protection impact assessment ("DPIA") under the GDPR. Under Article 35 (1) GDPR, where data processing operations are likely to result in a high risk to the rights and freedoms of natural persons, the data controller must carry out a DPIA before the commencement of data processing. Regarding the assessment of such risks, the controller must consider the type of processing when using new technologies and the nature, scope, context and purposes of the processing that may occur. The use of artificial intelligence for processing personal data will likely meet the legal requirement for completing a DPIA under Article 35 (1) GDPR, because AI is an innovative technological solution that may pose risks to individuals' privacy and data protection rights such as discrimination, bias or inaccuracy in the algorithms or unexpected outcome by data subjects.

Under Article 35 (4) GDPR, the Hungarian DPA established a list of processing operations which are subject to the requirement for a data protection impact assessment ("NAIH backlist")[6]. Under the NAIH blacklist, the use of new technologies for data processing or automated decision making producing legal effects or similarly significant effects requires a DPIA. These include the processing of large amounts of data obtained via sensor-equipped devices (e.g. smart televisions, smart household appliances, smart toys, etc.) and transferred through the Internet or other channels, and such devices providing data on the characteristics of the financial status, health condition, personal interests, trustworthiness or conduct, residence or movement of the natural person, and such data form the basis of profiling.

2.6 Data minimization

The GDPR also expects from controller to comply with data minimization. Within the context of the use of algorithms, data minimization means that only personal data that is adequate, relevant and limited to what is necessary for the purpose may be processed. According to the DPbDD Guidelines, this means that the controller must predetermine, which features and parameters of processing systems and their supporting functions are permissible regarding data processing. Within the context of designing and using algorithms, the controller is expected to avoid data processing when this is possible for the relevant purpose and the controller must also limit the amount of personal data collected to what is necessary for the purpose.

2.7 Storage limitation

[6] https://naih.hu/list-of-processing-operations-subject-to-dpia-35-4--gdpr.html; Last visited on 19 September 2020

The storage limitation principle says that the controller must ensure that personal data is kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed. Practically, the algorithm's operator must determine what data and length of storage is necessary for the purpose of data processing and the operator must be able to justify why the period of storage is necessary for a given purpose.

3. CONSUMER PROTECTION AND COMPETITION

When shopping on the Internet, consumers have access to a bigger range of products and an enormous market of potential contract partners. However, by using search engines, the search engine and not the user decides what products are proposed to the consumer. The proposals often come about through artificial intelligence and do not have to correspond to the interest of the user.

It is not quite obvious which approach fits the legal issues raised by the use of search engines, digital comparison tools, personalised advertisements / offers (personalised targeting) with special regard to the question, whether the consumer needs to understand the logic used by search engines, DTCs and if the answer is positive, to what extent the consumer must have an insight in the operation of search engines, DTCs. Under the Hungarian regulatory framework, search engines, DCTs and personalised targeting based on consumer profiles might primarily be assessed as a factor potentially influencing the consumers' decision making process by limiting the range of available choices, therefore, it is the most likely outcome that this issue would be treated in the framework of UCP Act.

The existing regulation includes the fundamental legal requirements which enables the enforcement as regards personalised targeting. Competent authorities, however, meet a challenge how to investigate the technicalities of personalisation and provide proper evidence for the legal assessment. Beyond proceedings focused on particular market behaviours, authorities may play a significant role in facilitating awareness of consumers and self-regulation of market players.

3.1 Market power and the use of AI

Interplay between data, artificial intelligence and market power have not been yet assessed in the Hungarian legal practice. General market tendencies which show that leading digital sectors tend to be leading sectors also in AI and use of AI has the potential to accelerate shifts in market share, revenue and profit. As for effect on competitive conditions, role of algorithms cannot be separated from the access to the data which serve as an input to algorithmical analysis (e.g. health care data) and the advantages available may simultaneously depend on both factors. Further, AI algorithms might change the nature of the concerned goods / services (e.g. new fields of personalised health care services are getting available resulting also from AI based research and analytics methods) and the transformation may reach and change the general mindset of the given industry as well. Therefore, due to the complexity of the issue, a case-by-case analysis is required.

Algorithms often undertake important forecast decisions and the contract negotiations on the internet while the customer functions as an observer. Autonomous algorithmic agents or autonomous software agents being present in the economy raise several questions, which can be linked to the contracting parties' private autonomy: (i) how to interpret in legal context the autonomy of software agents, whether they can take individual, stand-alone decisions (which do not fall in the category of automatised decision making); (ii) what are the potential risks and benefits of cooperation between people and software agents in economic decision making, (iii) how can network risks rooting in the integrated operation of computers systems be treated.

Following the above thread, it has to be assessed whether contracting party is in the position to decide whether or not any software agent should be involved in decision making, and if the decisions are left to algorithms, is there any requirement / benchmark how accurate they must be. Further, supervision of human and algorithm cooperation can be considered as a key issue, how can and should the human participant be able to intervene in the decision-making process. These issues may even let us draw the conclusion that the focus of investigation

ought to be re-directed from restriction of private autonomy to re-definition the concept of private autonomy to fit the transformation of the economic environment.

3.2 Algorithmic collusion

Algorithms often flexibly set prices of products on the Internet. If different companies are using the same or similar algorithms to set their prices, it might lead to intentional or unintentional price collusion. It is questionable whether companies should be required to disclose the functionality of their algorithms to make the process of price setting more transparent, because transparency in price setting may have anti-competitive effects, such as price fixing.

Digital businesses increasingly use algorithms in their price setting and such pricing algorithms can monitor pricing information by competitors. The increased transparency of such tools (its structure, workings etc.) and sharing publicly such competitively sensitive information may be considered illegal if this may lead to tacit collusion regarding price setting. However, if the user of the algorithm must provide an explanation that no collusion occurred, then the company may be required by the Competition Authority to disclose the functionality of the algorithm that its price setting complies with the law.

Up to now, Hungarian legal practice did not lay down clear principles how to differentiate between algorithm's collusion on their own (i.e. algorithmic collusion) and the use of code to enforce collusion (i.e. collusion by code), and market tendencies indicate that intermediary players, such as platforms may also be involved in algorithmic collaboration. Existing cartel rules might apply to such market relationships as well and fulfil the regulatory purpose if the challenges of detection and prosecution are met.

If use of algorithms deliberately allows undertakings to collude with the aim to raise the prices, such behaviour may be considered as unlawful from antitrust point of view. There are obvious cases, as for instance sharing pricing algorithms with competitors is a rather clear-cut infringement, but there may be more complex situations where coordination of parallel behaviour is taking place without the market players' performing any explicit communication.

According to the general antitrust logic, a low level of market transparency may offer opportunity to the cartel members to "cheat" the cartel system and to entice consumers away from their competitors. Thus, cartels usually monitor competitors' actions in order to shorten the period in which the cheating cartel member can use its strategy, and if revealed, deviations from the cartel rules are followed by sanctions of the cartel system. Use of price algorithms, as tools can contribute to the growth and/or sustenance of market transparency since deviation from agreed prices can be identified within seconds and the cheating member can face real-time sanctioning interventions.

3.3 Consumer discrimination in pricing

It is common for online platforms that they may discriminate among consumers regarding pricing any that platforms apply dynamic pricing structures based on customer segmentation. In practice, this means that the consumers will see different prices depending on the browser type and browsing history, type of end user device, number and timing of website visits, geographic location, and similar user behaviour data. There are common strategies to avoid such price discrimination and dynamic pricing, such as

- blocking IP address and geographic location data or by using VPN which permits the change of IP / geographic location;
- blocking the placement of third-party tracking cookies on the end user device;
- using price comparison websites and conducting search for more information;
- changing the end user device, or browser type for doing the search for a product and for performing the purchase, because first time customers likely become more benefits than returning buyers.

Further, use of personalised prices may also depend on other product / service characteristics. Among others, a potentially relevant categorisation can be based on the level of difficulty of consumers' information search prior to taking their transactional decisions. As for goods, at which consumers can typically rely on their prior

experience or can collect direct information on all essential features before taking their transactional decisions (i.e. search goods), personalised pricing can be subject to further assessment, provided that unjustified discrimination between the consumers is not taking place. As regards experience goods and credence goods, where accurate prior evaluation of the product / service as compared to personal needs is more difficult or even impossible to the consumers, consumers are obviously not in the position to compare and assess personalised prices.

In some countries, some markets (e.g. health product, health care services) belong to the regulated sectors, and to some products and services regulated prices are defined. In such markets, for instance, it can be worth to consider if personalising of prices can be introduced if the aspects of personalisation can be properly regulated and the consumer can have relevant and comprehensible information on personalisation methods.

3.4 Online sale restrictions

According to the CJEU's recent practice[7] it can be legal for manufacturers to prohibit the sale of their products on certain platforms in order to protect the product's image. "*Article 101(1) TFEU must be interpreted as meaning that a selective distribution system for luxury goods designed, primarily, to preserve the luxury image of those goods complies with that provision to the extent that resellers are chosen on the basis of objective criteria of a qualitative nature that are laid down uniformly for all potential resellers and applied in a non-discriminatory fashion and that the criteria laid down do not go beyond what is necessary. Article 101 (1) TFEU must be interpreted as not precluding a contractual clause, such as that at issue in the main proceedings, which prohibits authorised distributors in a selective distribution system for luxury goods designed, primarily, to preserve the luxury image of those goods from using, in a discernible manner, third-party platforms for the internet sale of the contract goods, on condition that that clause has the objective of preserving the luxury image of those goods, that it is laid down uniformly and not applied in a discriminatory fashion, and that it is proportionate in the light of the objective pursued, these being matters to be determined by the referring court.*" One of the conclusion of the judgment is that in case of luxury goods the protection of a brand image can sufficiently require a selective distribution system. The CJEU also stressed that its judgment in Pierre Fabre case is in line with the Coty judgment: the prohibition on all online sales of (even luxury) products remains prohibitive as it would be detrimental for the final consumers as well. However, there is no relevant Hungarian legislation or practice in this matter.

Manufacturers likely would also prohibit distributors from advertising the manufacturer's products on search engines, but this practice is very likely illegal. The European Commission fined Guess EUR 39,821,000 for restricting retailers from online advertising and selling cross-border to consumers in other Member States ("geo-blocking"), in breach of EU competition rules.[8] The Commission has found in its investigation – among others - that Guess' distribution agreements restricted authorised retailers from using the Guess brand names and trademarks for the purposes of online search advertising. Guess revealed this infringement beyond the cooperation with the Commission. The Commission decided that this was a restriction by object, however the retailers of Guess were able to sell online. Based on the Commission's decision it may not be legal for manufacturers to prohibit distributors from advertising the manufacturer's products on search engines because the distributors won't be able to effectively generate traffic to their own websites by means of online search advertising. There is no relevant Hungarian legislation or practice in this matter.

4. ENFORCEMENT

In Hungary, the HCA is in charge for the enforcement of the UCP Act (i.e. the Hungarian implementation of the Directive 2005/29/EC of the European Parliament and of the Council of 11 May 2005 concerning unfair business-to-consumer commercial practices in the internal market) if the unfair commercial practise materially distorts

[7] CJEU, C-230/16, *Request for a preliminary ruling under Article 267 TFEU from the Oberlandesgericht Frankfurt am Main (Higher Regional Court, Frankfurt am Main, Germany), made by decision of 19 April 2016, received at the Court on 25 April 2016, in the proceedings*, [ECLI:EU:C:2017:941], pt 6.

[8] EU Commission Comp. DG, Case AT.40428, *Commission Decision of 17.12.2018 relating to proceedings under Article 101 of the Treaty on the Functioning of the European Union and Article 53 of the Agreement on the European Economic Area,*

competition. Pursuant to the Hungarian Constitution, the enforcement of data protection rules is the exclusive competence of the Hungarian DPA being the supervisory authority of Hungary under Article 51 (1) GDPR. The HCA and the Hungarian DPA have a cooperation agreement[9] and these authorities discuss cooperation between these two authorities.

The HCA generally recognizes that data protection is part of "consumer welfare", because consumers consider the privacy aspects of online products as a significant product characteristic. In the Google Allo case (Vj/88/2016, closed with Commitment Decision), the HCA investigated whether consumers received the information necessary for an informed decision on Google's the data processing activity. In its decision, the HCA considered that data processing is an essential aspect of Google's products and that the consumer's informational self-determination right has not only privacy, but also market / competition aspects. Accordingly, the HCA acknowledged that the non-transparent nature of data processing may be a relevant aspect in the consumer's transactional decision.

Even if privacy law enforcement is the competence of the Hungarian DPA, to the extent data protection is part of the consumer / customer welfare and the breach of data protection provisions (such as privacy related transparency / information provisions) constitute an unfair commercial practice against consumers, the HCA adopted a policy to intervene and enforce unfair competition rules. The HCA has not yet applied the antitrust rules on social networks and similar online providers' data processing activities.

[9] https://www.gvh.hu/pfile/file?path=/gvh/egyuttmukodesi_megallapodasok/gvh_egyuttmuk_NAIH_GVH_2015_03_13&inline=true; Last visited on 19 September 2020