MCT 4009 EMERGING TECHNOLOGIES AND THE LAW

elsa

The European Law Students' Association

MALTA

ABOUT ELSA

ELSA Malta is a distinguished member of the ELSA International network, comprising over 50,000 students from more than 350 law faculties across Europe. The organization is deeply committed to upholding the values enshrined in its motto - "A just world in which there is respect for human dignity and cultural diversity" - and strives to achieve this mission in all its activities.

Founded in 1986, ELSA Malta is recognized as a prestigious student organization by the Senate of the University of Malta. Its primary aim is to represent all law students in the University and provide them with a diverse range of opportunities.

ELSA Malta offers various events throughout the academic year that cater to the needs of law students of all ages, providing them with an excellent opportunity to expand their legal knowledge across various topics in the Law Course. Additionally, these events can prove to be of great value to students from other faculties as well.

Furthermore, ELSA Malta also strives to promote international understanding and cooperation by fostering cultural exchange and encouraging students to participate in international projects, conferences, and competitions. By engaging in such activities, ELSA Malta seeks to equip its members with valuable skills and experiences that will help them become responsible and active citizens of the global community.

DISCLAIMER

Please note that the student notes provided by ELSA Malta are intended to supplement your own notes and independent study. These notes may contain errors or omissions, and we cannot guarantee their accuracy or completeness. While these notes may act as a tool to enhance your understanding of the material covered in class, we advise against relying solely on them in preparation for examinations or assignments. It is crucial to attend all classes, review the assigned readings, and take your own notes.

ELSA Malta cannot be held responsible for any consequences that may arise from the use of these notes, including poor academic performance or misunderstandings of course content.

By accessing and using these notes, you acknowledge and agree to these terms and conditions.

ACKNOWLEDGMENTS

ELSA Malta President: Alec Carter

ELSA Malta Secretary General: David Camilleri

Treasurer: Jake Mallia

Writer: Emma de Gabriele

MCT4009 - The Law of Emerging Technologies

Introduction

Understanding the regulation of emerging technologies necessitates a grounding in fundamental legal principles before delving into specifics. Emerging technologies have a transformative effect on our accustomed practices, requiring us to reference traditional phenomena to discuss them effectively. Rather than solely focusing on the latest advancements like AI, it is essential to also consider established technologies.

Engaging in the legal and regulatory aspects of emerging technologies demands significant effort, involving not only addressing legal issues but also shaping societal attitudes towards these phenomena.

As a general field of law, the European law of emerging technologies is rather broad and keeps expanding. In terms of legislative activity, the EU law of electronic commerce that began as a concentrated effort is continuously expanding. This includes in relation to the size of such pieces of legislation: the original Electronic Commerce Directive is ten pages, whereas the Digital Services Act, its successor in part, is around 200 pages. This not only reflects the volume and proliferation of technologies, but also underscores the fact that the complexity surrounding digital technologies has become more abundant.

The Law of Electronic Commerce

This is a very broad umbrella term which encompasses many different phenomena from internet transparency to platform regulation.

Currently, electronic commerce is governed by the **Electronic Commerce Directive, Directive 2000/31**. While this came into force in 2000, the majority is still in force with no plans to be amended. This is a testament to the success of the directive, as well as to the specific kind of regulation – regulation which is principle-based. Since the individual principles are not very detailed but only express the conceptual framework of how the legislator wants to see commerce transactions, it has significant longevity and it continues to apply, despite negotiations in its regard beginning in the mid-1990s. The enduring relevance of this instrument is attributable to this approach with the legislator foreseeing the growth of online business and its likely diversification and thus avoided tying the legislation to specific business models at the time of enactment, enabling flexibility.

Although the name implies that the directive mostly regulates electronic transactions, the law goes beyond that, making the title a slight misnomer. In fact, we note that parts of it regulate general behaviour in digital spaces, the most characteristic being the regulation of platforms including Google Search Engine, ChatGPT, Wikipedia, Instagram, YouTube etc.

When analysing the Electronic Commerce Directive, it is important to note that there remain other pieces of EU legislation that are important and which trickle into our understanding, especially the law of consumer protection. Therefore, the following pieces of legislation are important:

1. **Directive 2011/83: The Consumer Rights Directive.**
   This includes provisions mainly on the transparency and delivery of goods.

2. **Directive 2019/770** & **Directive 2019/771: Twin Regulations on Consumer Protection.**
   These tackle the substance of certain electronic transactions, namely, the sale of goods and the supply of digital content. They are more substantive as they unify compliance standards for goods and services in the digital environment, as well as the available remedies when compliance has not been achieved.

3. **Directive 1999/93** & **Regulation 910/14**: **Electronic Signatures and e-IDAS Regulation.**
   Such set standards for electronic signatures, seals, timestamps and electronic documents, aiming to facilitate secure electronic transactions and enhance trust in digital interactions within the EU.

Consumer protection, and therefore B2C transactions, is the only area of civil law where the EU has a clear mandate. In fact, in relation to B2B and C2C transactions, it is Member States with the mandate to regulate such.

Overall, the EU is widely regulated as a global internet regulator due to its vast market of 550 million people. This substantial market size empowers the EU to dictate to companies and businesses that to access this market, they must adhere to the rules and safeguards established by the Union.

Definitions and the Scope of the Electronic Commerce Directive

This directive primarily targets commercial transactions. However, to grasp its full scope, as is necessary with all EU legislation, we must acquaint ourselves with specific definitions. It's worth noting that the directive's language dates to 2000, therefore, contemporary equivalents will be offered to reflect the modern digital landscape.

What is the Purpose of the Directive?

In this regard, we consider **Article 1(1)** which provides the scope of the directive:

> *This Directive seeks to contribute to the proper functioning of the internal market by ensuring the free movement of information society services between the Member States.*

In one form or another, all EU actions aim to enhance the operation of the internal market. This directive seeks to encourage digital transactions by simplifying the operations of digital platforms and service providers across the EU. To grasp the legislator's strategy for achieving this goal and promoting electronic transactions, it is crucial to comprehend the definition of an *information society service* as it falls directly within the scope of the directive to regulate such services.

While it aims to incentivise doing business online, it simultaneously puts in place certain safeguards for the average user which are complimented by consumer protection law. In European electronic commerce law, there is a constant balancing exercise between incentivising digital business models and protecting those who lack power in those spaces. The EU is aware that the more technology advances, the greater the risks posed to users which increases the fundamentality of this balancing. Thus, because of the directive, the internet experienced by EU citizens is vastly different compared to foreign counterparts.

Subject Matter Scope of Application and Information Society Services

Upon reviewing the directive, it becomes apparent that information society services lack precise definitions under **Article 2(a)** wherein reference is made to another directive:

> *'Information society services': services within the meaning of **Article 1(2)** of Directive 98/34/EC as amended by Directive 98/48/EC.*

However, the recitals of the legislation offer insight into the legislator's understanding of what constitutes an information society. Thus, we note how the recitals contextualise the content and aid the interpretation of the substantive articles:

1. Systematically – By establishing the context within the legislative framework
2. Teleologically – By elucidating the legislative intent and purpose behind specific terms or choices.

Therefore, although not legally binding, these recitals hold value as they illuminate the rationale behind the insertion of certain terms or provisions by the legislation.

Vis-à-vis information society services, we look to **Recital 18**:

> *Information society services span a wide range of economic activities which take place on-line; these activities can, in particular consist of selling goods on-line; activities such as the delivery of goods as such or the provision of services off-line are not covered; information society services are not solely restricted to services giving rise to on-line contracting but also, in so far as they represent an economic activity, extend to services which are not remunerated by those who receive them, such as those offering on-line information or commercial communications, or those providing tools allowing for search, access and retrieval of data; information society services also include services consisting of the transmission of information via a communication network, in providing access to a communication network or in hosting information provided by a recipient of the service; television broadcasting within the meaning of Directive EEC/89/552 and radio broadcasting are not information society services because they are not provided at individual request; by contrast, services which are transmitted point to point, such as video-on-demand or the provision of commercial communications by electronic mail are information society services; the use of electronic mail or equivalent individual communications for instance by natural persons acting outside their trade, business or profession including their use for the conclusion of contracts between such persons is not an information society service; the contractual relationship between an employee and his employer is not an information society service; activities which by their very nature cannot be carried out at a distance and by electronic means, such as the statutory auditing of company accounts or medical advice requiring the physical examination of a patient are not information society services.*

From this definition, we understand information society services to be any service offered in online and remote terms, even when it doesn't need to be paid for with money. Therefore, there are two important notions that emerge from this definition:

1. The emphasis on the economic nature of the activities. We consider here, how the emphasis is on an economic activity and not a commercial activity.
2. The fact that information society services are not solely restricted to services giving rise to online contracting but also extend to services which are not remunerated. It is particularly impressive that the drafters in the late 1990s pre-empted the internet economy and caught a business model that was popularised over ten years after the recital was drafted: social media.

The economic nature and the absence of a remuneration requirement are connected concepts, so to speak. When the EU legislator mentions an economic activity, it encompasses any activity generating economic outputs, even if not directly compensated. This distinction holds

importance particularly in online contexts where many actions do not involve payment but still yield economic results. It is noteworthy that while individuals often perceive themselves as users online, the structure of the internet effectively makes them the product, as their online activities generate economic value making it an economic activity.

The following are some examples of activities that form part of information society services:

- Selling goods online.
- Search engines.
- ChatGPT and AI platforms.
- Video conferencing services.
- Cloud applications.
- Mobile apps.
- Subscription services.
- Wikipedia.

This illustrates the extensive and inclusive subject-matter scope of the directive, encompassing all activities conducted online, whether paid for or not. Any activities that produce any economic outputs and that happen online, which is a very low threshold are regulated by the directive and therefore, every online platform operating within the EU must adhere to the obligations in the directive.

In this regard, we consider the judgement **Sortiris v. Papasavvas (C-291/13)** which notes that services which are not remunerated directly by the recipient but by income generated by advertisement posed on a website are also included in this regard.

Subjective Scope of Application

This considers who is regulated by the directive and we consider both the offering and receiving parties.

In terms of offering parties, we consider service providers. The definition of a service provider is contained in **Article 2(b)**.

> *Any natural or legal person providing an information society service*.

Immediately, we note that both natural and legal persons can be service providers. Therefore, it shouldn't be taken for granted that only a company or a foundation may be a service provider. An example of an individual acting as a service provider is when Person A shares their hotspot with Person B. This makes Person A a service provider and a mere conduit. A person creating a website, or a Facebook page also is a service provider. The definition of a service provider is quite broad and presented in a very generous manner, similar to an information society service.

In terms of those on the receiving end of services, we distinguish between the recipient of a service and a consumer.

Article 2(d) defines the recipient of a service as:

> *Any natural or legal person who, for professional ends or otherwise, uses an information society service, in particular for the purposes of seeking information or making it accessible.*

Once again, this is quite a generous definition.

Article 2(e) then defines consumers as:

> *Any natural person who is acting for purposes which are outside his or her trade, business or profession*.

There are certain profound differences between recipients of a service and consumers. As established through the definition, a legal person can never be considered a consumer. This means that every time a legal person is at the receiving end of an online service, they are the recipient of a service, as opposed to a consumer. The fact that a consumer may always only be a natural person is something which has been clarified many times. Additionally, we note that the two experience very different legal treatment under law with there being vastly more protections for consumers the recipients of the service are not entitled to.

As a result of the vaster protections and the legal weapons this title affords, it is important to identify how one qualifies as a consumer. Whether a person is a consumer or not is dependent upon their level of experience and sophistication within a specific transaction as the legislation is constantly trying to protect the weaker socio-economic party. Therefore, the deciding criteria are experience and sophistication and has nothing to do with gaining financial assets or power. For example, if Person A were a very successful football player and comes to Malta on holiday and stays in a hotel that doesn't generate half what he earns, Person A is still considered to be a consumer since those running the hotel have far more sophistication and experience in hotel transactions and in the hotel business compared to him, making them the more powerful party.

We question what the situation is when it comes to **dual-purpose contracts**. As noted, a consumer is only such if the activity they are engaging in and the reason behind such engagement is outside their trade, business or profession. However, when dealing with dual-purpose contracts, a person engages in a contract for both professional and personal reasons, raising doubts as to whether such can be deemed a consumer or not. These situations are often not clear cut. An example of this would be Person A, being a professional film critic, paying for a Netflix subscription both for his own enjoyment but also to help him access films to review.

Therefore, the question is raised, how do we legally classify these people as they stand in the middle of being a recipient of a service and a consumer, as they cannot be both at the same time since such is contradictory. In delving into this exercise many questions are raised:

- Is it fair for the person engaging for a partly professional reason to be considered the weaker party nonetheless? This is interesting because likely, despite the professional element, the service provider is more sophisticated than the user regardless. Consider a situation where a TikTok personality begins to monetise their account and begins to turn it into their careers. Despite this, overwhelmingly, TikTok remains the more sophisticated party.
- Should the fact that one is making use of the service for professional elements mean there should be more gravity and therefore, that they should be entitled to less protections?

Initially, this dilemma was settled by the CJEU, yet now, we are given an indication as to the solutions within the law itself. Here, we take into consideration the **Consumer Rights Directive – Directive 2011/83/EU** in particular **Recital 17**:

> *The definition of consumer should cover natural persons who are acting outside their trade, business, craft or profession. However, in the case of dual-purpose contracts, where the contract is concluded for purposes partly within and partly outside the person's trade and the trade purpose is so limited as not to be predominant in the overall context of the contract, that person should also be considered as a consumer.*

Through this recital, we firstly note that we must consider the specific contract in question. In case of a dual-purpose contract, it implores us to make an assessment as to what the predominant purpose of the contract is. If the predominant purpose is a professional purpose, then the individual engaging in the contract cannot be considered to be a consumer and is the recipient of a service. Thus, in such cases, for a person to remain a consumer, the professional element must not be the predominant element or motivator of the contract but must be "*so limited*" that it is practically negligible.

This understanding finds its basis in previous CJEU jurisprudence that too maintains that in situations like this, for a person to remain a consumer, they must prove that the professional element of the contract is so limited that it is negligible in the overall scheme of things. It is fair to say that this has a strict interpretation considering that legally classifying someone as a consumer bears significant consequences as they become entitled to legal protections which are strong deviations from the legal norm and thus, should not be handed out indiscriminately.

It is also important to consider, that **Recital 17** cannot be regarded in a vacuum and must be taken contextually in relation to CJEU case-law as it is, in and of itself, a codification of that which was promulgated through CJEU judgements, one of which being **Johann Gruber v. Bay Wa AG (C-464/01)**:

> *Where a contract has a dual purpose, the predominant purpose, whether private or business, must be ascertained. Since the dividing line between private and business supplies [was] difficult to distinguish [in this case], the court found that the seller had had no way of ascertaining objectively whether one or other purpose predominated at the time when the contract was concluded so that, given the uncertainty, the contract was to be regarded as a consumer contract.*

Additionally, the case-law maintains that a contract which is 60% personal, and 40% professional is not sufficient for one to remain a consumer, despite the wording of the recital which speaks about the "*predominant*" element. The professional element must be negligible in order to justify the status of a consumer. Yet, we maintain that it isn't easy to determine whether the personal or professional element has the greatest bearing in the contract.[1]

We also question whether one can **lose their status as a consumer**. Here, the element of time must be taken into consideration. Human transactions are dynamic and change over time and therefore, we question whether over time, one might lose their legal status or change their legal status within the same transaction. This question was brought before the CJEU in the case **Schrems v. Facebook Ireland Ltd (C-311/18)**. The facts of the case are as follows:

> As a university student, Schrems opened a Facebook account and began using it as a typical user. In this situation, Facebook was a service provider and Schrems was a consumer. By creating the account, the plaintiff entered into an electronic contract for the provision of electronic services. Along the way, the individual noticed that he would often mention something and got related ads on Facebook as to similar content and determine that Facebook was surveying him. From that moment on, he decided to dedicate his life to bringing service providers such as Facebook to courts for violations of the GDPR and consumer protection laws, thereby using their business models against them. He even set up a non-profit dedicated to this cause seeking to garner financial support for strategic cases to be taken against undertakings which endangered the right to data protection, he wrote books about his legal proceedings, gave lectures (some of which were remunerated) and registered several internet websites and blogs. Through all this, Schrems maintained a Facebook account. Undoubtedly, there was a qualitative change in behaviour and the way the platform was being used.

When Mr Schrems brought an action before the Regional Civil Court in Vienna seeking, *inter alia*, declaratory relief, an injunction prohibiting the use of his data for certain purposes, disclosure concerning the use of his data and damages, he claimed that he had the standing to bring the case on the basis of his own rights and similar rights which seven other users had assigned to him for the purpose of this action. He further claimed that they were "*consumers*" and therefore, as per **Article 16** of the **Brussels I Regulation**, the Viennese courts had

[1] Consider the understanding of dual-purpose contracts given in **Schrems v. Facebook Ireland Ltd (C-311/18)** on page 10.

jurisdiction since such ought to be based on the "*domicile of the consumer*". Here, **Article 15** defines a consumer contract as one that has been entered into "*for a purpose which can be regarded as being outside his trade or profession*."

The question arose as to whether Schrems was still considered to be in a consumer contract with Facebook. The Regional Civil Court claimed he wasn't since he was also using Facebook for professional purposes and therefore, he lost the privilege of jurisdiction based on the domicile of the consumer. This moved through the Austrian legal system till it ended up before the Supreme Court of Austria which subsequently referred two questions for preliminary ruling by the CJEU, the first being of primary interest in this regard:

> *As per **Article 15** of Regulation No 44/2001, can the title of "consumer" be lost if, after a comparatively long use of a private Facebook account, the user begins to profit from the actions related to the platform?*

Therefore, the CJEU needed to acknowledge the element and influence of time on the quality and character of a transaction. When considering the meaning of "*consumer*" under Regulation 44/2001, the court maintained that this notion must be strictly interpreted and construed since the ground of jurisdiction based on the weaker party is an exception to the rule of *actor sequitur forum rei*.

Firstly, it stated that reference had to be made to the position of the person concerned in the contract, having regard to the nature and object of that contract and not to subjective situation of the person concerned. Secondly, the court explained that the special jurisdiction rules for consumers, only apply to contracts "*concluded outside and independently of any trade or professional activity or purpose, solely for the purpose of satisfying an individual's own need for private consumption.*" This was because the special rules were designed to protect weaker parties, and such protections are unwarranted in cases of contracts for trade or for professional activities. The court clarified that where the contract was concluded for a purpose that was partly concerned with a person's professional activity, **Articles 15** and **16** of Regulation No 44/2001 only applied if the link between the contract and the trade or profession was so slight as to be marginal and, therefore, had a negligible role in the context of the supply in respect of which the contract was concluded.

The court, when applying these rules in the context of contracts for services of a digital social media network which are intended to be used over a long period of time, noted that subsequent changes in the use which is made of those services must be considered. The court highlighted the element of time when analysing the developments of the relationship between the contracting parties. Ultimately, it was noted that social network users can only rely on the special rules on jurisdiction in bringing a case in such circumstances where they can show that their predominantly non-professional use of those services had not become predominantly professional. Teleologically, this can also be expanded to consider all the other benefits at law enjoyed by consumers.

Nevertheless, the court was careful to clarify that the fact that an individual acquired expertise or knowledge in the field covered by the services under contract, or that they had given assurances to represent the rights and interests of users of those services cannot deprive them of their status as a consumer. If they were to be so deprived, the court noted that:

> *... this would have the effect of preventing an effective defence of the rights that consumers enjoy in relation to their contractual partners who are traders or professionals, including those rights which relate to the protection of their personal data*.

In light of the above, the court held that the notion of consumer for the purposes of **Article 15** of Regulation No 44/2001 must be interpreted as meaning that the activities of publishing books, lecturing, operating websites, fundraising and being assigned the claims of numerous consumers for the purpose of their enforcement, did not entail the loss of a private Facebook account user's status as a consumer. Therefore, the CJEU held that a privacy rights activist and campaigner could not lose his status as a consumer in his contractual relationship with Facebook because of his activities in campaigning and litigating against the company. The court recognised this consumer status even though Schrems failed to fit into the standard, tradition idea thereof, indicating that a person's status as a consumer must be assessed on a case-by-case basis and that such a legal status cannot be transferred universally in all other legal relationships that a person enters into in the future.

Many believe that the reason behind this judgement was to ensure that Facebook was not given the ability to abuse such case law for their own purposes in capriciously deciding who qualifies as a consumer or not based on the way they are using the platform. Nonetheless, the CJEU still gave merit to Facebook's argument that a legal relationship can change over time within the same transaction. This has strong implications as it meant that one may start as a consumer in a transaction but not remain a consumer throughout the course of the same transaction.

Qualities and Principles of the Electronic Commerce Directive

Here, we consider namely the following principles:

1. The Principle of the Country of Origin – **Article 3**
2. The Principle of No Prior Authorisation – **Article 4**
3. Information Requirements – **Articles 5, 6** and **7**
4. Treatment of Electronic Contracts – **Articles 9, 10** and **11**
5. Liability of Intermediaries – **Article 12, 13, 14** and **15**, however, this has now been repealed and replaced by the **Digital Services Act**.

The Electronic Commerce Directive establishes a legal framework for electronic commerce within the EU. It aims to facilitate the free movement of goods and services in the digital single market by harmonising certain legal aspects of electronic commerce across EU Member States. It works to stimulate digital transactions with the legislator having aimed for its policies to make it easier for businesses to get online and safer for consumers to trust, thereby ensuring responsible and safe operations. This includes protections and recourse for consumers and recipients of services, with the former having their protections reinforced by other instruments outside of the Directive. This entire scheme manifests itself through the aforementioned pillars.

The Principle of Country of Origin

Here, we turn to **Article 3**, i.e. the internal market clause, which outlines this principle of country of origin. As we shall see, it is not entitled the internal market clause arbitrarily. In fact, it exists to make it easier for companies to operate online within the common market.

> *Each Member State shall ensure that the information society services provided by a service provider established on its territory comply with the national provisions applicable in the Member State in question which fall within the coordinated field.*
>
> *Member States may not, for reasons falling within the coordinated field, restrict the freedom to provide information society services from another Member State.*
>
> *Paragraphs 1 and 2 shall not apply to the fields referred to in the Annex.*
>
> *Member States may take measures to derogate from paragraph 2 in respect of a given information society service if the following conditions are fulfilled:*
>
> a. *The measures shall be:*
>
> i. *Necessary for one of the following reasons:*
>
> - *Public policy, in particular the prevention, investigation, detection and prosecution of criminal offences, including the protection of minors and the fight against any*

incitement to hatred on the grounds of race, sex, religion or nationality, and violations of human dignity concerning individual persons.

- *The protection of public health.*
- *Public security including the safeguarding of national security and defence.*
- *The protection of consumers, including investors.*

ii. *Taken against a given information society service which prejudices the objectives referred to in point (i) or which presents a serious and grave risk of prejudice to those objectives.*

iii. *Proportionate to those objectives.*

b. *Before taking the measures in question, and without prejudice to court proceedings, including preliminary proceedings and acts carried out in the framework of a criminal investigation, the Member State has:*

i. *Asked the Member State referred to in paragraph 1 to take measures and the latter did not take such measures, or they were inadequate.*

ii. *Notified the Commission and the Member State referred to in paragraph 1 of its intention to take such measures.*

Member States may, in the case of urgency, derogate from the conditions stipulated in paragraph 4(b). Where this is the case, the measures shall be notified in the shortest possible time to the Commission and to the Member State referred to in paragraph 1, indicating the reasons for which the Member State considers that there is urgency.

Without prejudice to the Member State's possibility of proceeding with the measures in question, the Commission shall examine the compatibility of the notified measures with Community law in the shortest possible time; where it comes to the conclusion that the measure is incompatible with Community law, the Commission shall ask the Member State in question to refrain from taking any proposed measure or urgently to put an end to the measures in question.

Therefore, this article establishes that online service providers are subject to the rules of the Member State in which they are established and not to the rules of the Member States where the service is accessible, even in the jurisdictions of these other States. Therefore, Member States in which the online service provider provides its services must therefore refrain from

applying national legalisation to its activities and may only restrict the freedom to provide information society services from another Member State under very clearly elucidated circumstances.

This was introduced to address the situation of businesses being subjected to the application of foreign law which would become difficult should the business face regulatory issues in other jurisdictions, i.e. to tackle the regulatory burdens that businesses would suffer if they had to comply with all the laws of all the jurisdictions that they would operate in. It, therefore, aims to incentivise entrepreneurship and to make it easier for people to set up online businesses. It is important because one of the major hurdles to setting up an online company in the EU was the fact that one must deal with 27 different jurisdictions all which have different legal systems and compliance standards. Through this provision, the legislator has removed that concern and burden associated with international online operation by removing the regulatory requirements, to a certain extent. This burden was especially lifted from the shoulders of start-ups and SMEs

Therefore, as it stands, there remains a requirement to comply, but companies need only to comply with the laws of the Member State in which they are established. This enables them to disregard the laws of the other 26 Member States so long as they comply with the one of where they are established, promoting more online activity.

One of the major issues which arises pertains to how this operates in relation to private international law (PIL), both for users as well as for the service provider. We note that the field of law which dictates what law is applicable in a transaction with international elements is private international law and not the law contained in the directive. This is acknowledged in the directive itself through **Article 1(4)**:

> *This Directive does not establish additional rules on private international law nor does it deal with the jurisdiction of Courts.*

Therefore, the rules of country of origin are not PIL rules, yet PIL remains meaningful for electronic transactions. We note that ultimately, PIL is influenced by principles enshrined in the directive, including the principle of country of origin. In this regard we consider the **eDate Advertising Case (C-509/09)** and the **Martinez Case (C-161/10)**, on privacy and personality infringement vis-à-vis **Article 5(3)** of Regulation No 44/2001, now **Article 7(2)** of the Brussels I Recast Regulation. This marked the first time the CJEU was tasked with analysing the relationship between PIL and the Directive as well as address how to combine PIL and country of origin rules.

Here, a question as to which court had jurisdiction and for what damage arose in relation cases of alleged infringement of personality rights by means of content placed online. With it, there was the consideration as to whether the platform accused of breaching personality rights should be judged according to the laws of a different Member State or whether the electronic

company should only be concerned with the laws of the country of their establishment due to the principle of country of origin.

Vis-à-vis jurisdiction, both cases were predicated on **Article 5(3)**, now **Article 7(2)**, which notes that jurisdiction is based on "*the place where the harmful event occurred or may occur*." To solve this, the CJEU analysed existing case-law, including the seminal **Shevill Case (C-68/93)** which dealt with defamation through a magazine article. It had held that on the basis of **Article 5(3)** a case may be instituted either:

- Based on where the actual damage arose for the entire amount of damages, i.e., before the courts of the contracting State of the place where the publisher of the defamatory publication is established
- Based on where the actual damage was felt for the amount of damage therein felt, i.e., before the courts of the contracting State where the publication was distributed and where the victim suffers injury to reputation.

This is known as the mosaic principle. The CJEU agreed with Mr AG Cruz Villalón that this applies also to other media and means of communication that can infringe personality rights. However, it was noted that in case of the internet, different measures needed to be taken into consideration given its ubiquitous nature and the opportunity for accessibility throughout the Union. In fact, content put online can be consulted by an unlimited number of internet users, thereby reducing the usefulness of the criterion relating to distribution and the harm caused as a result. Therefore, it was determined that a third ground must be introduced, granting the plaintiff the right to institute a case:

- Based on where the damage was felt for all the damage, i.e., before the courts of the Member State in which the centre of interests of the plaintiff are based, most often conforming to his habitual residence.

In relation to the question as to which law should apply, the CJEU confirmed that in this case, the principle of country of origin is not a PIL rule and thus, has no authority to determine the applicable law in a case with a foreign element. The law applicable must always be determined using traditional PIL rules, in this case through the rules of the Member States since such was excluded from application under the Rome II Regulation on non-contractual obligations. Nonetheless, the CJEU confirmed that while PIL determines the applicable law, nonetheless the principle of country of origin plays a part considered that any foreign court applying a foreign law must take into account this privilege that electronic companies are afforded as a result of the law of their country of establishment. Therefore, the principle of country of origin still influences the application of the chosen law through PIL rules as a form of compromise.

This applies as follows: There exists a French electronic platform on which the personality of a Greek individual has been infringed. A dispute is brought before Greek courts with the national PIL rules determining that Greek law is applicable. Because of the benefit of **Article**

3(1), the French-established platform is empowered to argue that despite the applicability of Greek law to the dispute, French law must apply to the extent that it is more favourable t the platform. Here, the Greek judge is not offered discretion and must apply the more favourable French laws as the law of the country of establishment - the moment the electronic company evokes the principle of country of origin, the judge must respect.

This also could apply to contracts as per the following example: A person established in Italy buys a car from an electronic commerce business established in Croatia. In the contract, there existed a choice of law pointing to Italian law. After 7 months it arises that there exists a defect. According to Italian law, the seller is liable for all defects to the product that may appear within two years of delivery as opposed to under Croatian law where liability ceases after six months. According to PIL rules, the applicable law would be Italian law, but the Croatian company is able to protect itself from liability by claiming that Croatian law is more favourable, reducing the amount of time it can be found liable and must be applied.

Thus, while the principle of country of origin doesn't dictate the jurisdiction or the applicable law of a dispute, with such being regulated by PIL rules, it still influences the application of such. Consequently, this becomes a significant determining factor when the decision as to where an electronic company will be established is being made: the decision tends to be made depending on which laws are more favourable to its operations.

The Principle of No Prior Authorisation

This is outlined under **Article 4** of the Directive:

> *Member States shall ensure that the taking up and pursuing of the activity of an information society service provider may not be made subject to prior authorisation or any other requirement having equivalent effect.*
>
> *Paragraph 1 shall be without prejudice to authorisation schemes which are not specifically and exclusively targeted at information society services, or which are covered by Directive 97/13/EC of the European Parliament and of the council of 10 April 1997 on a common framework for general authorisations and individual licenses in the field of telecommunications services.*

This stipulates that an electronic commerce company which is established in a Member State and which operates in all other Member States of the Union doesn't need to obtain the authorisation from every Member State in order to operate there.

Therefore, if a person from Finland wishes to establish an electronic company there, such company can immediately operate in all other Member States and target clients outside of Finland with no other Member State may subject this undertaking to any form of prior authorisation. If a Member State blocks the platform and demands individual authorisation, there is an infringement on this principle.

Information Requirements

The information requirements demanded of companies in digital markets through **Article 5** are essential for transparency's sake. Transparency is essential in the digital space performing a dual function of:

1. Protecting consumers/users – Without the minimum information provided by this platform, it is unlikely that an individual will enter into a transaction with such a party as there is no way to know who is actually being dealt with. It can be dangerous when one is unable to assess the risk, especially should something go wrong. Should the user require something to be fixed or compensated, the information contained under **Article 5** should be made available or there will be a lack of confidence.

2. Detracts individuals from engaging in criminal or harmful behaviour as anonymity isn't allowed – By having these requirements, the EU creates an online market that can be supervised. If a person has to present their identity, they are far less likely to engage in criminal behaviour as they will be made to suffer the consequences thereof.

Thus, the need to establish mechanisms of transparency come from the idea that for people to trust electronic transactions, they must be transparent in order for people to make informed decisions as to whether to enter into them or not.

Article 5 highlights the general information to be provided as follows:

> *In addition to other information requirements established by Community law, Member States shall ensure that the service provider shall render easily, directly and permanently accessible to the recipients of the service and competent authorities, at least the following information:*
>
> *a. The name of the service provider.*
>
> *b. The geographic address at which the service provider is established.*
>
> *c. The details of the service provider, including his electronic mail address, which allows him to be contacted rapidly and communicated with in a direct and effective manner.*
>
> *d. Where the service provider is registered in a trade or similar public register, the trade register in which the service provider is entered and his registration number, or equivalent means of identification in that register.*
>
> *e. Where the activity is subject to an authorisation scheme, the particulars of the relevant supervisory authority.*

f. As concerns the regulated professions:

i. Any professional body or similar institution with which the service provider is registered.

ii. The professional title and the Member State where it has been granted.

iii. A reference to the applicable professional rules in the Member State of establishment and the means to access them.

*g. Where the service provider undertakes an activity that is subject to VAT, the identification number referred to in **Article 22(1)** of the sixth Council Directive 77/388/EEC of 17 May 1977 on the harmonisation of the laws of the Member States relating to turnover taxes — Common system of value added tax: uniform basis of assessment.*

In addition to other information requirements established by Community law,[2]Member States shall at least ensure that, where information society services refer to prices, these are to be indicated clearly and unambiguously and, in particular, must indicate whether they are inclusive of tax and delivery costs.

We note that the service provider may be a legal or natural person and that the remained of the requirements apply regardless of the denomination

In accordance with **Article 5(1)(a)**, the name of the service provider is to be outlined. This doesn't refer to the name of the website but to the name of the service provider itself – i.e. the company or person behind the website.

Article 5(1)(b) stipulates the need for there be a listed geographic address of the service provider on the website. While this can also be a postal address, it must be the same as the place of incorporation and must refer to the place where the service provider is actually established.

In relation to **Article 5(1)(c)** we take into consideration the **Deutsche Internet Versicherung (C-298/07)**. Here, a consumer association decided to bring a lawsuit against the named company. Their compliant was that their website didn't comply with **Article 5(1)(c)** since they didn't provide a telephone number, only an email and a contact form. The association complained that the electronic contact form was equivalent to an email and ignored the directive's requirement that contact details must enable "*rapid*", "*direct*" and "*effective*" communication. They argued that the only way this can be achieved is through the provision

[2] See further Article 10 of the Directive which provides further requirements

of a telephone number. The CJEU was questioned as to whether there existed another way for communication to be rapid, direct and effective.

It concluded that a telephone number is not the only means of communication satisfying these requirements. It noted that in the modern day, there are different ways to communicate and so long as the consumer/user gets an answer as soon as possible through the contact means provided, then the method is sufficient to satisfy the requirements under **Article 5(3)**. Additionally, the court noted that by law, a human agent isn't necessary for rapid, direct and effective communication – it could also be a chatbot so long as they are equipped to effectively help users solve their problems.

> ***Article 5(1)(c)*** *of Directive 2000/31 on certain legal aspects of information society services, in particular electronic commerce, in the internal market, must be interpreted as meaning that a service provider is required to supply to recipients of the service, before the conclusion of a contract with them, in addition to an electronic mail address, other information which allows the service provider to be contacted rapidly and communicated with in a direct and effective manner. This information does not necessarily have to be a telephone number but may be in the form of an electronic enquiry template through which the recipients of the service can contact the service provider via the internet, to whom the service provider replies by electronic mail except in situations where a recipient of the service, who, after contacting the service provider electronically, finds himself without access to the electronic network, requests the latter to provide access to another, non-electronic means of communication.*

This case consolidated the benchmark for this requirement to be complied with: communication mechanisms must be rapid, direct and effective, with there being no default mechanism that is compliant. In fact, it could also be that a telephone number doesn't satisfy these criteria. Therefore, to comply with this provision, a company must provide an electronic mail address at minimum but also include another means of communication, generally a direct messaging form, for example WhatsApp or Messenger.

Article 5 doesn't stipulate where service providers are to keep this information, be it all in one space or on the website. We note that under German law, when the directive was transposed, they included the obligation to keep all **Article 5** information in the same section of the website. This is one of the few, if not the only Member State that outlines requirements over and above what is called for in the EU instrument.

Further, we consider that **Article 5** is not the only article to regulate information requirements and depending on the circumstances, we may need to take into consideration additional provisions. While **Article 5** establishes general information requirements, highlighting that regardless of the type of activity being provided, this information must always be available, **Article 10** outlines further information that must be given by the service provider when an electronic contract is entered into:

In additional to other information requirements established by Community law, Member States shall ensure, except when otherwise agreed by parties who are not consumers, that at least the following information is given by the service provider clearly, comprehensibly and unambiguously and prior to the order being placed by the recipient of the service:

a. *The different technical steps to follow to conclude the contract.*

b. *Whether or not the concluded contract will be filed by the service provider and whether it will be accessible.*

c. *The technical means for identifying and correcting input errors prior to the placing of the order.*

d. *The languages offered for the conclusion of the contract.*

Member States shall ensure that, except when otherwise agreed by parties who are not consumers, the service provider indicates any relevant codes of conduct to which he subscribes and information on how those codes can be consulted electronically.

Contract terms and general conditions provided to the recipient must be made available in a way that allows him to store and reproduce them.

Paragraphs 1 and 2 shall not apply to contracts concluded exclusively by exchange of electronic mail or by equivalent individual communications.

The law makes it clear that the information stipulated in **Article 10** must be provided "*in addition to other information requirements*", referring to those listed under **Article 5**. Such information is specific only to those situations where a contract is being concluded, otherwise it doesn't apply, increasing the thresholds and requirements. However, we recall that almost everything done online constitutes a contract.

Article 10(1)(a) outlines the different technical steps required to conclude the contract. This enables people to effectively interact with the system.

Article 10(1)(b) highlights that the service provider must state whether the contract will also be filled in by them and whether it will be accessible. This is for the user to know whether they will have a chance to see the terms and conditions again, which is especially important if something were to go wrong. If the user is precluded from revisiting the contract, then it would be in their best interest to download the document and thus, be furnished with such information.

Article 10(1)(c) deals with the mechanism through which input errors can be arranged such as putting in the wrong address or adding too many of the same item to the cart. Firstly, we

question whether this affects the validity of the contract and whether the consumer or user is bound by the initial agreement since the website cannot know how many of the products the user intended to buy. Generally, the contract is valid and binding upon purchase, but if there is a mistake, it is voidable with the user having the option to go to court to declare the part of the contract in excess as invalid. This is, however, difficult to prove in court which is why the law stipulates that service providers must give the technical means to identify and correct errors to avoid a situation in which a contract will be voidable for a reason of mistake in expression of will.

All the information above discussed duties designed for the Electronic Commerce Directive alone. However, should one of the parties to a contract be a consumer, the Consumer Rights Directive must also be looked at. Specifically, we consider **Article 6** which includes further information requirements when dealing with consumers. In fact, **Article 6** of the Consumer Rights Directive supersedes **Articles 5** and **10** of the Electronic Commerce Directive when dealing with consumers and ensures that service providers comply with all requirements under all three articles. This applies to distance or off-premises contracts, and therefore to an online contract.

In this regard, **Article 6(1)(h)** is of particular importance:

> *Before the consumer is bound by a distance or off-premises contract, or any corresponding offer, the trader shall provide the consumer with the following information in a clear and comprehensible manner: where a right of withdrawal exists, the conditions, time limit and procedures for exercising that right in accordance with **Article 11(1)**, as well as the model withdrawal form set out in Annex I(B).*

This notes that the internet service provider must inform the consumer whether a **right of withdrawal** exists as well as the conditions, time limits and procedures for exercising this right. We consider that a consumer who buys online, always has the right to withdraw, as per **Article 9**, which a service provider is obliged to inform him about:

> *Save where the exceptions provided for in **Article 16** apply, the consumer shall have a period of 14 days to withdraw from a distance or off-premises contract, without giving any reason, and without incurring any costs other than those provided for in **Article 13(2)** and **Article 14**.*

The exceptions under **Article 16** to this rule include, for example, service contracts after the service has been fully performed if the performance has begun with the consumer's prior express consent and with the acknowledgement that he will lose his right of withdrawal once the contract has been fully performed by the trader; the supply of goods or services for which the price is dependent on fluctuations in the financial market which cannot be controlled by the trader and which may occur within the withdrawal period; the supply of goofs made to the consumer's specifications or which are clearly personalised, *inter alia*.

Therefore, the principle applies that if one buys something online, they are able to withdraw from the contract and return the item within 14 days from the day of delivery and in doing so, the money is refunded. This applies to electronic commerce mainly because there is risk purchasing online without actually seeing the product and therefore, the law provides an opportunity for the consumer to feel and see the product face-to-face. This doesn't apply if the consumer damages the product and wishes to return it as such is not a lawful exercise of the right to withdraw from an electronic contract. Thus, the law allows you to inspect the product but not to damage it with the obligation put on the consumer to return the product in a condition to be able to sell it to someone else.

Liability of Intermediaries

This is now considered under the Digital Services Act and no longer under the Electronic Commerce Directive.

Deceptive Design Patterns or Dark Patterns

Deceptive design patterns are commonly referred to as 'dark patterns', a term originating not from law but from computer scientists. To understand what these are, we must keep in mind the relationship between law and information technology, noting that this form of law is very interdisciplinary, and the manner in which the law operates in a societal context vis-à-vis these technological developments.

Harry Brignull is a design ethicist which refers to an individual who focuses on human computer interface, i.e., how one interacts with websites and applications, *inter alia*. He speaks about interface design as the means through which we interact with that that has been designed. He further defines dark patterns as "*tricks used in websites and apps that makes one do things they don't mean to, like buying or signing up for something*." Therefore, we are referring to how online experiences may sometimes be subject to deception and manipulation by virtue of the manner in which these platforms are designed.

A more recent definition came from Marthur et al (2019):

> *[Dark matter refers to] interface design choices that benefit an online service by coercing, steering, and/or deceiving users into making decisions that, if fully informed and capable of selecting alternatives, they might not make and are culpable for causing financial loss, tricking users into sharing large amounts of personal data, or inducing compulsive and addictive behaviour.*

Therefore, dark patterns refer to those design choices that reflect what the online provider wishes to see from the user, but not something which is necessary in the user's best interest. In fact, such may even harm them. These are facilitated through websites and platforms making use of deceptive and manipulative techniques aimed to serve their commercial interests.

In common parlance, this notion of compulsive and addictive behaviour is used often, especially in relation to social media. In fact, social networking sites, such as Facebook and Instagram, are designed in such a way to generate obsession and addiction. This has gotten to the point that today we speak about the attention economy – an economy based on grabbing the attention of the audience. However, the fact that this addiction has become so commonplace is not by chance. It all stems from design choices: designing a more interactive and addicting platform that will steer and coerce users will increase engagement, creating a commercial and financial advantage for the business behind it.

Sometimes, it doesn't only relate to the addicting way a platform is designed. Taking the example of Facebook, we consider that a user has no option to use Facebook without agreeing to be targeted with behavioural advertising. Traditionally, when we speak about surveyance, we talk about the government surveying a population to maintain and control them. Yet, in the world of electronic commerce, the surveyance becomes commercial –

through the tracking and monitoring of a user's behaviour via technological systems, such systems can analyse the patterns one makes use of to generate an accurate image of them based on their online clicks to target them with behavioural advertising intended to influence and impact decision-making processes. Additionally, with the coming of age of AI, we note that these advanced systems can also infer information about users.

At this junction it is important to make certain comments about 'users'. Here, users refer to either data subjects and to consumers, which may or may not refer to one in the same person: many times a person would be both a data subject in data law terminology and a consumer in the terminology of consumer protection law. Therefore, we see that data protection law and consumer protection law both play a role in this regard. These two areas of law interact and overlap, with the core legislation of the former being the General Data Regulation (GDPR) where the person whose data is being processed is referred to as a data subject. Take the following example: Person A opens a Facebook account. As mentioned, there is no option to use Facebook without it tracking your data. This means that through the person's interactions with the social platform it tracks their behaviour making them a data subject and Facebook a data consumer. At one and the same time, Facebook is also a service and when one signs up, they agree to the terms and conditions of the contract and since it's a B2C relationship, it makes the person a consumer. Should an instance of unfairness arise in Person A's relationship with Facebook, we note that the relationship may be regulated by either data protection law or consumer protection law. While the authorities are different, their areas of competence overlap.

Consumers are increasingly facing dark patterns because many-a-time online user interfaces are designed specifically to deceive them. Here, the focus is on the design element. When referencing design, we speak about an element of intentionality and understand the relationship between law and the system architecture, i.e. the code. The idea between law and code is very important. In the offline arena, we consider that the architecture of a building determines how one interacts with the building: where one enters and exits from and where one walks. Thus, the architecture regulates one's behaviour in the building. In the online environment, architecture is called code, and this computer code regulates one's behaviour online. Take the following example into account: Person A wishes to read an online newspaper article yet access to such requires the user to log in to their account. This is the result of the programming of a system which grants access rights only if one has a subscription. In such a way, code is enforcing the law – someone who produces the content has a right to demand payment when others access it and therefore, this design element ensures that no one who hasn't paid can gain access to it. The rule is enforced through a system coded in the computer system.

We note how a system, theoretically can be designed in any manner, yet the GDPR speaks about data protection by design which means that one is under the obligation to design a system that is privacy friendly. For example, if a user is signing up for a social media account, data protection by design means that when one signs up, the default privacy setting should be that sharing from that account is restricted to sharing amongst a close group of

friends and not universal. While this obligation is incumbent upon system designers, systems can also be designed to deceive and manipulate users and because this aspect of technology has gained prominence, this terminology has started to be used in various contexts, despite not being legally binding.

In association, we also consider the use of unfair practices. One of the clear examples is tracking in this regard. Tracking online activity happens across websites and may sometimes bring about negative consequences. While it may be convenient in certain cases, specific forms of tracking may lead to situations where users are unaware of the extent that they are being deceived and manipulated and ultimately, this strikes at their decision-making abilities. This links to the notion that the ultimate threat of technology and in particular AI systems is that we have lost our autonomy.

The term 'dark patterns' is a very broad term used to describe may situations. While some authors have tried to create a form of taxonomy thereof to make sense of the situations where dark patterns are made use of, it is easier to consider individual examples.

Example I - Cookie Consent Mechanisms and Dark Patterns

The first example that can be brought of deceptive designs and patterns is the cookie consent mechanism made use of by websites and applications.

A cookie refers to small systems installed in one's terminal that enable user tracking across the platform. Here, we distinguish between essential cookies and optional cookies. The former are those cookies that are mandatorily required and are essential for the operation of a website. A clear example in this regard is the basket on Amazon – without this feature and without Amazon remembering what was put in the basket, one would be unable to make a purchase. These are not usually problematic. However, websites tend to go much further than this to collect far more personal data and track users to a much greater extent.

In the EU, enabling cookies requires one to consent to the placing of optional cookies on one's terminal, therefore, making use of the 'opt in' obligation as opposed to the 'opt out' method of consent. This is not required for essential cookies as such are necessary for the website or application to function.

When entering a website, a user will be presented with a cookie consent mechanism. From studies conducted by psychologists that use computer technology and AI to analyse human behaviour to see how it can be manipulated or controlled, we note that when presented with a large green button, one is more likely to click it and alienate other options. If there is a large green button presented encouraging a user to 'Accept Cookies', it steers users into accepting as opposed to 'Rejecting. Through this design, the interface is nudging one to behave in a particular way which is often, not in the best interests of the user, but is in the interest of the online provider as through that choice, they become free to monitor online behaviour which can be used to facilitate targeted advertising.

This indicates that while speaking about data protection and consumer protection, there is a very strong economic value to our personal data.

This design is made worse in the case where a 'Reject' option isn't even presented but only a 'Managing Options' or 'More Information' button is included. While it could be that by clicking the button, one finds an option to opt out of this kind of tracking, it is much harder to navigate and get out of as opposed to the option to opt out being presented in the form of a 'Reject' button on the consent mechanism portal. This is a form of cognisant bias whereby one is being led to accept tracking. While in principle, the option to opt out is being provided in accordance with EU law, the design of the website is done in such a way as to nudge the user into sharing their personal data to the advantage of the online service provider.

In this example, it is likely that one will seek a remedy under data protection law.

Example II – Facebook GDPR Pop-Up and Dark Patterns

When dealing with the GDPR pop-up on Facebook, we note that users are presented with the option to accept and continue with tracking and such tracking includes from third-party websites. To avoid this, Facebook requires users to go into Manage Data Settings to turn off ads based on data from third parties. If the user simply clicks 'Accept and Continue', the setting is automatically turned on. This is not privacy by design and default, as is mandated at law through the GDPR, as it is requiring users to take extra steps to stop this form of tracking.

To be compliant with data privacy law, Facebook must make the automatic setting for third-party tracking off, giving the option for users to opt-in. However, it does the opposite and therefore, infringes the GDPR.

Example III – All Personalised Ads Turned On By Default

Example IV – Promising Rewards or Threatening Punishment

In this case, a scenario would arise whereby a user will be given a form of 'punishment' for making the choice which is not the preferred choice of the online service provider. Take the example of Facebook, a user can be told that by not accepting the terms and conditions of Facebook including the cookies, they will not be able to use Facebook. This is a form of punishment as the platform then encourages you to delete the account. Many people who do not wish to lose the information they have accumulated over the years on the site accept cookies for this reason and therefore, the platform isn't giving one a choice but is coercing the user into acceptance.

Example V – Forced Registration and Dark Patterns

In such a scenario, a user will be forced and coerced to register to make a purchase. Logically, there is no real reason why a service provider should require registration to make a purchase but in doing so, the website or application can gain access to the information that is typically required to make an account including one's name, address and other personal data.

Example VI – Confirm Shaming and Dark Patterns

In this scenario, a user is given two options and is somehow made to feel ashamed for the option they choose. Hence, the user is being steered into taking the decision that the service provider wants one to make. This is all about the design – the way that one's choices are presented will make one feel as though they ought to take a certain decision which is a form of online manipulation or coercion.

Example VII – Nagging and Dark Patterns

This arises in those cases where a user is being presented with the options 'Later' and 'Try Now' without being offered the choice of saying 'No'. A nagging dark pattern is a way to coerce one into a particular form of action because if a user is continuously presented with an option and notifications repeatedly are sent to their device, to get rid of it, it is likely that it will be agreed to. Here, the question arises as to why consent is being forced without the option to deny it.

Example VIII – Stylised Example of a Hard to Cancel Dark Pattern

This arises typically when users sign up for a service such as Spotify or Netflix where a monthly subscription is involved, and the cancellation of that subscription is much more complicated than signing up for it. While there is no commitment to sign up for the subscription, the fact that the method of cancellation is much more onerous means it was designed in such a way as to make it harder to cancel, meaning subscribers are less likely to cancel.

None of this is coincidental. These are intentional design choices made by the business that offers products or services in this manner based on what they known human beings' cognitive biases and weaknesses to be to coerce us into taking a particular decision or to behave in a particular manner.

Example IX – Countdown Timers and Dark Patterns

This form of dark pattern arises whenever a platform includes a timer or tells users that there is only one item left in stock. These tactics create a sense of urgency resulting in the user hurrying up and taking a rushed decision. Often, these countdown timers are fake and are introduced solely to create this false sense of urgency. If a company runs a promotional deal for a limited time, to be lawful it must be a genuine discount for the time stipulated.

Example X – Hidden Costs, Drip Pricing and Dark Patterns

Hidden costs arise when one uses a platform and sees an item at a price which one deems worthwhile. By the time the user goes through all the stages of the purchase and is at the final point of the pre-contractual stage, one is informed that there are also taxes, handling fees and other hidden fees which makes the initial enticing offer not so worthwhile anymore. The issue is that once a person has gone through all the hurdles, despite the issues, they are likely to go ahead with the purchase anyway. This is a form of baiting and one pays more than they originally thought.

Example XI – Stylised Example of Activity Notifications and Dark Patterns

This arises when a website indicates that a specific amount of people have viewed the product in the last 24 hours. There is no indication of whether this is true, and it could be very misleading. This could also arise when it states that X amount of people have the item in their cart.

Example XII – Trick Questions and Dark Patterns

One of the main examples is "*Are you sure you want to cancel your order?*" If the user went through the whole process to cancel, this question serves only to manipulate the user into not cancelling. Another example is when a user is asked to tick the box if they wouldn't like to receive communications. Generally, this operates the other way around and a person must tick if they want to receive. These options are presented in a manner which intend to trick or mislead the user.

Example XIII – Price Comparison Prevention and Dark Patterns

Here, a service provider will give the user options to select from, such as different plans, but it makes it very hard to compare the price of the options. This kind of design is usually very intentional seeing as the functionalities are listed in a way that makes it difficult to compare whether the increase in price is worthwhile for the user. Confusion means people are more likely to sign up for the more expensive option on the presumption that it better and will give more value.

Example XIV – Misdirection and Dark Patterns

Here, the website provides the impression that one is meant to pick a particular option, with the option pointed towards being more beneficial for the operator. For example, if an airline asks a passenger to continue checking in or to pay for an upgrade and points them towards selecting the upgrade.

Example XV – Hidden Advertising and Dark Patterns

This is often referred to as disguised advertisement whereby a user is given the impression that they are going to do one thing, but in reality, are taken to another site where the initial thing they tried to undertake is being offered at a price. One of the central tenants of consumer protection law is transparency – the service provider should not deceive consumers. Consumer law has several provisions which deal with information requirements including knowing who is being dealt with, understanding the product being purchased and its functionality and identifying consumer rights generally.

While there is nothing inherently wrong with advertising, it should nonetheless be clearly marked as such. Sites such as Google are in accordance with consumer protection law as they make it clear when the first results that come up after a search are there because they have been paid for as advertising. This is essential.

Example XVI – Scarcity and Dark Patterns

Here, the service provider wishes to create the sense of urgency that the product or service won't be available much longer to encourage the user to purchase it.

Example XVII – Forced Action and Dark Patterns

Here, the service provider doesn't give the user a choice and notes that in order to access content or a service it must perform an action, either signing up to a free trial or something similar.

Taxonomy of Dark Patterns

Category	Name of dark pattern	Description	Source
Forced action	Forced registration	Consumer forced to register or tricked into thinking registration necessary	Bösch et al. (2016[21])
	Forced disclosure / Privacy zuckering	Consumer tricked or forced into sharing more personal information than desired	Bösch et al. (2016[21]); Gray et al. (2018[23]); Brignull (n.d.[11])
	Friend spam / Social pyramid / Address book leeching	Manipulative extraction of information about other users	Bösch et al. (2016[21]); Gray et al. (2018[23]); Brignull (n.d.[11])
	Gamification	Certain aspects of a service can only be "earned" through repeated use of service	Gray et al. (2018[23])
Interface interference	Hidden information	Important information visually obscured	Gray et al. (2018[23])
	False hierarchy	Visual prominence given to firm's preferred setting or version of a product	Gray et al. (2018[23]); Mathur et al. (2019[24])
	Preselection	Firm-friendly default is preselected (e.g. more expensive or less privacy-protecting option)	Bösch et al. (2016[21]); Gray et al. (2018[23])
	Misleading reference pricing	Price shown as a discount from a misleading or false reference price	OECD (2019[3]); CMA (2022[31]); EC (2022[29])
	Trick questions	Intentional or obvious ambiguity (e.g. double negatives)	Gray et al. (2018[23]); Mathur et al. (2019[24]); Brignull (n.d.[11])
	Disguised ads	Consumer induced to click on something that isn't apparent advertisement	Gray et al. (2018[23]); Brignull (n.d.[11])
	Confirmshaming / Toying with emotion	Emotionally manipulative framing to make consumer select a particular option	Brignull (n.d.[11]); Gray et al. (2018[23]); Mathur et al. (2019[24])
Nagging	Nagging	Repeated requests to do something firm prefers	Gray et al. (2018[23])
Obstruction	Hard to cancel or opt out / Roach motel / Click fatigue / Ease	Asymmetry in ease of signing up/opting in to a product or firm-friendly choice versus cancelling/opting out	Brignull (n.d.[11]); Dapde (n.d.[26]); Gray et al. (2018[23]); Forbrukerrådet (2018[27]); Mathur et al. (2019[24])
	(Price) comparison prevention	Frustrates comparison shopping regarding price or content	Gray et al. (2018[23]); Mathur et al. (2019[24]); Brignull (n.d.[11])
	Immortal accounts	Account and consumer information cannot be deleted	Bösch et al. (2016[21])
	Intermediate currency	Purchases in virtual currency to obscure cost	Gray et al. (2018[23])
Sneaking	Sneak into basket	Item consumer did not add is in cart	Brignull (n.d.[11]); Gray et al. (2018[23]); Mathur et al. (2019[24])
	Hidden costs / Drip pricing	Costs obscured or disclosed late in transaction	Brignull (n.d.[11]); Gray et al. (2018[23]); Mathur et al. (2019[24]); OECD (2019[3])
	Hidden subscription / Forced continuity	Unanticipated or undesired automatic renewal of a service	Brignull (n.d.[11]); Gray et al. (2018[23]); Mathur et al. (2019[24])
	Bait and switch, including bait pricing	Consumer is offered product or price different from that originally advertised	Brignull (n.d.[11]); Gray et al. (2018[23]); OECD (2019[3])
Social proof	Activity messages	Indications about other consumers' actions, which may be misleading or false	Mathur et al. (2019[24])
	Testimonials	Statements from other consumers regarding a product, which may be misleading or false	Mathur et al. (2019[24])
Urgency	Low stock / High demand message	Indication of limited quantities of a product, which may be misleading or false	Mathur et al. (2019[24])
	Countdown timer / Limited time message	Indication of an expiring deal or discount, which may be misleading or false	Mathur et al. (2019[24])

Source: Consolidated taxonomy adapted from Luguri and Strahilevitz (2019[223]; 2021[25]). Sources for individual taxonomies containing each dark pattern are indicated in the table.

It is unlikely that there will ever be a definitive and complete taxonomy of dark patterns since new ones are constantly emerging and the list we have currently not being future-proof. Further, these lists all reflect authors' objectives and depend greatly on the inclusion and

exclusions of the study being undertaken, each reflecting the understanding or definition of dark patterns adopted by the researcher.

We note that the dark patterns shown above are all visible. They pertain to the notion of human computer interaction which is multidisciplinary and takes into account societal influences as well as scientific backing. However, we consider the rising phenomenon of 'darkest patterns' since there are examples which cannot be seen and identified. For example, we consider the development of technology, especially AI powered technology and how such has the power to manipulate users at the sub-conscious level, such as through subliminal advertising which isn't so easily identifiable. In fact, the effectiveness of some dark patterns may be driven by their subtlety and difficulty of detecting them, which may in turn relate to a consumer's prior experience with the dark pattern, vis-à-vis its intrinsic difficult of people detected or its general pervasiveness.

Further Expansion into Dark Patterns

The term 'dark patterns' was originally coined by Brignull who was not a lawyer but a design ethicist. As noted, this term refers to a wide variety of practises commonly found in online user interfaces that lead consumers to make choices that may not be in their best interests, including by exploiting cognitive and behavioural biases and heuristics. They typically seek to get consumers to give up more money, personal data or attention time than desired. In this way they are inextricably linked to an underlying business model, even if user interface designers may often bare no ill intent. They generally share one or more end-goals with the ultimate purpose of increasing business revenue and therefore, designers are often incentivised to develop user interfaces that perform well in terms of metrics relevant to the business model. This even includes the use of aggressive dark patterns because while such may drive some consumers away, the increased revenue from the bulk of the consumers on whom they are effective will still incentivise their use and result in profit-maximisation.

As we have seen, these are common on electronic commerce websites and apps, including those of major online platforms. Many, actually feature more than one dark pattern, particularly in relation to cookie consent notices which indicate high rates of violation of data protection laws.

The working definition being proposed by the OECD is as follows:

> *Dark commercial patterns are business practices employing elements of digital choice architecture, in particular in online user interfaces, that subvert or impair consumer autonomy, decision-making or choice. They often deceive, coerce or manipulate consumers and are likely to cause direct or indirect consumer detriment in various ways, though it may be difficult or impossible to measure such detriment in various instances.*

As noted, they cause substantial consumer detriment, generally lead to financial loss, significant privacy harms or psychological detriment, weaken competition, and while there isn't evidence yet suggesting that dark patterns triggering personal vulnerabilities are common, this may change with business' increasing data collection combined with machine learning techniques. These harms are likely to be cumulative where multiple dark patterns are employed at once and are interrelated. One of the main issues in this regard is that they disproportionately effect less educated consumers and children.

We also consider how by hindering consumers' ability to make free and informed choices, dark patterns impair consumer autonomy. Personal autonomy has been defined as the capacity to make one's own choices, by having the competency to do so and being able to authentically endorse the reasons for them. Dark patterns may compromise this autonomy to the extent that they lead consumers to make choices they ordinarily would not have made, all the while projecting the illusion that consumers maintain control. They further may cause structural consumer detriment by affecting consumers collectively through impacts on competition or trust in online business.

Unsurprisingly, critics associate the following harms with the use of dark patterns: lower autonomy, a reduction in over- all social and consumer welfare; an erosion of trust; increased insecurity; and unfair treatment among consumers while risking anticompetitive effects (if a sufficient market power exists). Furthermore, if unjust data-driven discrimination persists due to a data-grabbing dark pattern, individuals and groups can suffer persistent disadvantages; for example, the unfair consequences associated with algorithmic bias and reinforcement of the social advantages to the detriment of another. Thus, dark patterns distract from two of the central objectives of the European 'Union's digital single market: creating the right conditions and a level playing field for digital networks and innovative services to flourish and max-imise the growth potential of the digital economy.

The conclusion derived from the identification of these dark patterns was that interface design should be ethical and take into account both consumer rights and data protection standards. In fact, since it is unlikely that market forces will be able to address dark patterns alone and many times actually incentivise their use for competition purposes, consumer and data protection authorities have accordingly been taking action on the basis of laws outlining practices associated with many dark patterns and issuing guidelines to support business compliance. This includes when evidence arises of third-party entitles facilitating dark patterns, something especially prevalent in relation to social-proof activity notifications. We consider however, that disclosure and transparency measures are not sufficient in isolation to protect consumers from dark patterns.

Since it originally wasn't a legal term, the idea of 'dark patterns' is used in a very broad manner. For example, sometimes it is used to describe something which one doesn't like about an interface, but which isn't necessarily illegal per se. Therefore, not every instance of a dark pattern being used means that the service provider is in breach of the law, it could just be an annoying practice adopted by the service provider. This is the job of lawyers in this

field: to find the connection between the fact found in the online world and the translation of these ideas into legal terminology. However, if the company is engaging in a dark pattern and it ends up in a legal dispute and it arises that an illegal action was being engaged in, it then must be seen which law will provide a remedy against this activity. Aside from legal remedies, it is also important to consider that educational, technical and business initiatives to address dark commercial patterns are also needed.

Privacy, Data Protection and Electronic Commerce: Data Protection vis-à-vis Dark Patterns

In today's electronic commerce environment, data plays a pivotal role in shaping consumer experience and driving business strategies. With the advent of electronic commerce, the landscape of data collection has evolved significantly. This evolution not only empowers businesses to personalise marketing efforts but also raises important considerations about privacy, security and the ethical use of consumer data.

However, the concept of consumer profiling isn't a recent development and predates the rise of electronic commerce. Even in offline shopping experiences, businesses leverage various consumer studies to tailor our interactions. Loyalty cards and electronic payments further enable the collection and analysis of our shopping preferences, serving as a foundation for diverse marketing strategies, including prove discrimination tactics, i.e. understanding that people in a particular environment are willing to spend a certain amount to purchase a product and then selling the product for different amounts in different areas to maximise profit based on this information. These strategies are designed to influence our purchasing decisions and include, for example, placing products at eye level to increase visibility and likelihood of purchase or creating environments that encourage longer stays, which tend to lead to increased sales. These strategies are testable and therefore, easier to implement since they are more likely to result in success, which for the business generally means increased revenue.

However, more than offline commerce, electronic commerce needs information to operate optimally. Firstly, we note that there are many different types of online environments that facilitate this type of transaction and consumer relationship. These include, for example, sole-traders or online marketplaces like Amazon where a consumer can purchase directly from Amazon or from a third-party seller that uses Amazon as a platform to sell the product. In the latter scenario, a three-party relationship is created where the seller contracts with the consumer who purchases through the online marketplace.

Their need for information can be thought of as the flip side of the information that consumers require before making a purchase. We note that in consumer protection law, we place an important emphasis on transparency in consumer contracts, which is why we mainly concern ourselves with B2C relations. As a consumer, one needs information: from specificities about the product they wish to purchase, to costs, to shipping and delivery information, to information about the entity being contracted with, to the rights enjoyed under the contract, to the right of withdrawal etc. This enables the contracting to take place in a fair environment. Conversely, the trader also demands transparency from the consumer and requires information from the consumer in order to market and advertise their products in a more targeted and precise manner. This generally pertains to demographic data which includes traditional data, such as name, address and financial details of the purchaser and modern information including mobile, email address and social media handles.

As highlighted, to obtain this information, entities often engage in forms of consumer profiling. When such activities are being conducted in an offline environment, there is still a degree of anonymity that is achievable: despite CCTV and DNA testing, a person remains a face in the crowd and can pay in cash to remain faceless. However, online this is harder to achieve. Anonymity cannot be sought since websites require information such as credit card details, delivery details and access details for information. Some of this data is even given by one's device itself while a user is on the terminal. This is why there is the idea that consumers are being watched online.

Many websites use techniques to track and consider the number of accesses, the number of return visits and the browsing patterns of consumers. This means that when one accesses an online marketplace, there are techniques that can track what one is doing. This is done using cookies, through which web servers can store information on one's computer. Cookies refer to a program that is installed on one's computer terminal and every time the web server is accessed the server can recognised a return visitor, even without providing a name, surname or email, following which a person can be directly identified. Cookies enable the server to remember the information outlined above: user specific data and login information.

From the point of view of a trader, since the system keeps track of how often one revisits a site and also the user's browsing patterns thereon, this information may be placed and read by the server when one is visiting the site or by a third party whom a user has given permission to by accepting that their data will be shared to third-party entities, usually advertisers. Such enables the service provider and the third-party to build a profile of the accessing user from the accumulated information in the environment to predict that they are interested in and what they are more likely to spend money on so the interface can be presented in such a way so as to motivate a transaction or purchase decision.

NB. Issues related to privacy still arise even when websites have privacy policies. Even though such aren't mandatory, we see that may websites are electing to make use of them, even though they are not obvious to an average user, complex, open to misinterpretation, skewed and highly favourable to the website. These are often legally unenforceable and ignored by users.

In relation to the protection of personal data in electronic commerce, we note that all electronic commerce businesses in the EU using personal data are subject to the rules in the **General Data Protection Regulation (2016/679)** known as the GDPR. This is the primary law in the EU dealing with data protection and is the reason for the modernisation of this topic in the EU. While there are other instruments and additional rules covering electronic communications, such as **Directive 2002/58/EC** amended by **Directive 2009/136/EC**, also known as the ePrivacy Directive concerning the processing of personal data and the protection of privacy in the electronic communications sector, the GDPR is the main instrument. The aforementioned ePrivacy Directive was meant to undergo a revitalisation but

the legislator, for a number of reasons including controversy surrounding it, has chosen not to amend it since 2009.

Core Data Protection Principles in the GDPR

Firstly, it is important to distinguish between a 'data subject' and a 'data controller'. Under the GDPR, a 'data subject' refers to an individual who can be identified directly or indirectly, such as through identifiers like name, identification number, location data, online identifier, or factors specific to their physical, physiological, genetic, mental, economic, cultural, or social identity. In simpler terms, it's any person whose data is being processed. On the other hand, a 'data controller' is a person, entity or organisation that determines the purposes and means of processing personal data. This includes deciding how and why data is collected, what it's used for, and how long it's retained. Data controllers have legal responsibilities under the GDPR to ensure that personal data is processed lawfully, fairly, and transparently, and that data subjects' rights are protected.

Substantively, we consider **Article 5** which outlines the principles relating to the processing of personal data and the compliance mechanisms that must be adopted by interfaces of online applications:

> *Personal data shall be:*
>
> a. ***Processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency')***.
>
> b. *Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for achieving purposes in the public interest, scientific or historical research purposes or statistical purposes, shall, in accordance with* ***Article 89(1)*** *not be considered to be incompatible with the initial purposes ('purpose limitation').*
>
> c. ***Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation')***.
>
> d. *Accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that is inaccurate, having regard to the purposes for which they are processed, is erased or rectified without delay ('accuracy').*
>
> e. *Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public*

*interest, scientific or historical research purposes or statistical purposes in accordance with **Article 89(1)** subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation').*

f. Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality').

The controller shall be responsible for, and be able to demonstrate compliance with paragraph 1 (accountability).

Therefore, **Article 5** contains the core data principles. These are namely:

- Lawfulness
- Fairness
- Transparency
- Purpose Limitation
- Data Minimisation
- Accuracy
- Storage Limitation
- Integrity and Confidentiality
- Accountability

For the purposes of this discussion, it is pertinent to focus on those contained in **Article 5(1)(a)**, **Article 5(1)(c)** and **Article 5(2)** namely: lawfulness, fairness, transparency, data minimisation and accountability. This is because the principle of fair processes and transparency laid down in **Article 5(1)(a)** supported by the assessments of data minimisation and accountability under the other relevant articles serve as a starting point to assess whether design patterns actually constitute a 'deceptive design pattern'.

Article 5(1)(a) is a very comprehensive principle that contains the notions of lawfulness, fairness and transparency.

Lawfulness

To process data, through cookies or other devices, the controller must establish on what grounds data is being processed, i.e. the legal grounds on which the data is being processed. The GDPR operates in such a manner whereby data can only be lawfully processed if a legal basis can be identified. There are six alternative grounds listed in **Article 6(1)** of the GDPR, three of which are relevant within the context of electronic commerce, since the others

provide rules relevant to the public sector and electronic commerce is a private sector endeavour.

> *Processing shall be lawful only if and to the extent that at least one of the following applies:*
>
> a. ***The data subject has given consent to the processing of his or her personal data for one of more specific purpose**.*
>
> b. ***Processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract**.*
>
> f. ***Processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third-party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which requires protection of personal data, in particular where the data subject is a child**.*

These criteria provide a lawful basis for the processing of personal data.

Taking into account first **Article 6(1)(a)** which speaks about **consent** as a legal basis, we note that whenever the data subject has given consent to the processing of their personal data, the data controller has the legal grounds to process the data. Therefore, this ground is predicated on consent. Consent can be for a specific purpose or for multiple specific purposes with the key word being "*specific*". The data subject must know what the controller is planning on doing with their data, otherwise the consent given isn't valid.

While consent may seem simply, this is often not the case. In fact, **Article 4(11)** of the GDPR provides that consent means:

> *Any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by clear affirmative action, signifies agreement to the processing of personal data relating to him or her.*

This is further clarified by **Recital 32** that all these conditions must be cumulatively met in order for such to be considered as valid. In relation to freely given consent, **Article 7(4)** provides that "*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.*" Here, the law says when interpreting whether consent has been freely given, if a contract or service provider requires the data subject's consent for processing personal data that is not essential for fulfilling the contract's purpose, then this condition could raise questions about the freedom to consent. The GDPR aims to ensure that individuals are not pressured or compelled to

provide consent for data processing that goes beyond what is necessary for the fulfilment of the contractual obligations.

Some of the major problems of consent include:

- Users not informed: Many people consent without knowing what they are consenting to, especially considering that, as we have already mentioned, often privacy policies are difficult to understand yet contain important information as to what is happening to one's data.

- Certain websites and information service providers make the provision of their services conditional on the data subject consenting to tracking behaviour. This is being done by Facebook which doesn't allow a person who hasn't consented to being tracked to use its services. Thus, while Facebook might technically be a free platform it still comes at the cost of knowing that you are being tracked whenever you are using it. This is problematic because consent under the GDPR needs to be free and it seems that consent under the threat of withholding a service is not free as it is conditional on one being excluded from the service. Therefore, on the basis of **Article 7(4)**, Facebook cannot justify its processing activities on the basis of consent because they refuse to provide a service to anyone who doesn't fully consent to being tracked. Therefore, the use of the service is condition upon being tracked and thus, according to the GDPR, this Is not free consent.

Keeping in mind the fact that websites and applications are often designed to deceived or manipulate a data subject to provide consent to be tracked, when a service provider is purporting to base their data processing on consent as a legal basis, consent is considered to be freely given when it is not based on some form of deceit or manipulation to trick the consumer into providing it and more information than they wanted to share. Therefore, these deceptive patterns may actually run afoul of the GDPR.

We note that to process personal data there doesn't always need to be explicit consent. Through **Article 6** of the GDPR, various bases of consent are provided for, and a data controller can make use of any which one of them in order to process data, thereby by-passing the need to absolutely gain the consent of users. However, this only applies when any of the other lawful bases for tracking data are used and not when **Article 6(1)(a)** is being made use of as such requires consent given in satisfaction of the requirement that it is "*freely given, specific, informed and unambiguous*."

Another important notion of consent is the withdrawal thereof. **Article 7(3)** outlines that:

> *The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. Prior to giving consent, the data subject shall be informed thereof. It shall be as easy to withdraw as to give consent.*

Therefore, one of the qualities of consent as a lawful basis is that data processing on the basis of consent means that one has the right to withdraw their consent as easily as they gave it and from that moment on the processing of the data must stop. If there is no option of withdrawal of consent then such consent is not freely given and thus, consent cannot be used as a legal basis for justifying processing. In the case that we are dealing with a dark pattern whereby we are dealing with a hard to cancel dark pattern, this violates the GDPR since withdrawing consent must be as easy as giving it.

We also ought to take into consideration the notion of consent from a child's point of view which is becoming increasingly more relevant as more minors enter online spaces. Here, we take into account **Article 8** of the GDPR:

> *Where point **(a)** of **Article 6(1)** applies, in relation to the offer of information society services directly to a child, the processing of the personal data of a child shall be lawful where the child is at least 16 years old. Where the child is below the age of 16 years, such processing shall be lawful only if and to the extent that consent is given or authorised by the holder of parental responsibility over the child. Member States may provide by law for a lower age for those purposes provided that such lower age is not below 13 years.*

Thus, for the purposes of the GDPR, a child can consent at 16 but it also allows some flexibility at the Member State level to lower the age to a minimum of 13. The word "*may*" highlights this as a facultative obligation for which there is no requirement. This means that the age of 16 isn't actually harmonised across the EU with no such means provided for the logistics thereof. Therefore, while the default rule is that if an information society service offers a service to a minor, they must be at least 16 or their consent is subject to the authorisation of the person exercising parental responsibility, at a Member State level, states have the discretion to provide for a lower age of consent, provided this is not under 13. In Malta, the Data Protection Act brings this down to 13.

Further, we note that there exist other ancillary obligations in relation to consent, such as **Article 12** of the GDPR which requires controllers to take appropriate measures to provide any communication related to data subject rights, as well as any information in a concise, transparent, intelligible and easily accessible form, using clear and plain language. As **Recital 39** notes on the principle of transparency, that this requirement is not limited to data protection notices or to data subject rights, but rather applies to information and communication relating to the processing of personal data. Data subjects should be made aware of the risks, rules, safeguards and rights in relation to the processing of personal data and how to exercise their rights in relation to such processing.

Article 6(1)(b) then outlines the legal basis of processing necessary to perform a **contract**. In such a situation, the data controller enters into a contract with the data subject and begins to process personal information on that basis, or else begins to process information prior at the

data subject's request. An example of this ground would be as follows: Person A purchases a physcial thing which means they need to leave an address for it to be delivered. In this context, the trader can rely on this ground of processing because the data being analysed is necessary for the performance of the contract. Without this information, the contract cannot be performed.

Another example pertains to Facebook, a company that is continuously involved in GDPR complaince battles. The company tried to argue that this ground could cover their processing of user's personal data, stating that the processing that they do is necessary for the performance of the contract entered into by consumer to use the social networking platform and services, the counter-performance of which is the agreement that the recipients of the service would be subject to behavioural tracking and advertising. This came after Facebook had already tried to use consent as an appropriate legal basis which was ruled out. The CJEU did not accept this reasoning because, inter alia, the term "*necessary*" denotes proportionality and must be interpreted more narrowly than Facebook attempted to define it since Facebook doesn't require to track us strictly to provide the service. This principle, in reality, is hard to transplant into a contractual relationship where a controller is processing massive amounts of personal data at the request of the data subject. The issue is as to how far a service provider can go to argue that the processing of data is necessary for the performance of the contract in order for it to be a legal basis for processing. This has become very controversial.

Finally, we take into account **legitimate interests**. Therefore, a legitimate interest pursued by a controller or a third-party, except when such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child. This is perhaps the ground most open to interpretation and thus, from a legal perspective is the most challenging ground since it incorporated this balancing act: that which is necessary for the legitimate interests of the controller, balanced against the interests of the data subject. This is generally a test assessed by judges when they weigh individual rights against public interests. The legitimate interests of the controller covers mundane interests like direct marketing, explicitly recognised in **Recital 47**.

Under the principle of 'lawful', Facebook as a controller was used as an example frequently because there is a long saga of legal proceedings being taken against them because they process data not in compliance with the GDPR which is illegal since they have a headquarter in Dublin and target individuals in the EU. This means they are subject to this regulation and must be GDPR compliant. They tried and failed to use all three of the aforementioned legal bases.

Around two months ago, Facebook informed its users in Europe that they could pay to use the services and not be tracked, i.e. either pay for the service or consent to behavioural advertising. This is because it argued it has no businesses model without one or the other, either a payment for the services or the analysis of user data. This is also currently being challenged by the NGO NOYB which is arguing that European should need to pay for their fundamental right to data protection included in the Charter of the EU as it opens the door to discrimination.

We still question what legal basis Facebook is using to process consumer data. While other websites were designed to be GDPR compliant and can use consent which is freely given, the model of Facebook precludes it from using consent. Whatever Facebook does to find a legal basis to process information, they have consistently been challenged. Mainly, they are being challenges by privacy activists. These activists would like to see the abolition of behavioural advertising as they believe it is intrusive of privacy, increases surveillance and is bad in terms of democracy and a free society, and therefore, consumers should have the option to opt out of intrusive and invasive methods of data collection. However, there exists the risk that soon, Facebook might have to be removed from European markets owing to this non-compliance, which may have negative political effects.

Fairness

Fairness is an overarching principle which requires that personal data shall not be processed in a way that is detrimental, discriminatory, unexpected or misleading to the data subject. If the interface has insufficient or misleading information for users and fulfils the characteristics of deceptive design patterns, it can be classified as unfair processing. This has served an umbrella function, and all deceptive design patterns would not comply with it, irrespective of other data protection principles. \

Transparency

Here, transparency means that the controller must provide information about what is being done with the data subject's personal data. This includes when they collect, process, store, test, share and analyse data. The data controller has an obligation to be transparent in this regard. This principle of transparency has a large overlap with the area of general accountability. Even though controllers have to protect certain sensitive business information towards third-parties, making documentation on processing accessible or recordable could help provide accountability which serves at the same time to ensure transparency towards data subjects.

All the data protection principles set out in **Article 5** are specified further throughout the GDPR. For example, in relation to transparency and the requirement that data be processed in a transparent way vis-à-vis the data subject, we note that the Guidelines on Transparency specify the elements of transparency as laid down by **Article 12**, i.e. the need to provide the information in a "*concise, transparent, intelligible and easily accessible form, using clear and plain language*." These guidelines also provide guidance on how to fulfil the information obligations under **Articles 13** and **14** regarding social media providers. **Article 13** outlines the information to be provided when personal data is collected from data subjects whilst **Article 14** stipulates the information to be provided where personal data has not been obtained from the data subject. Together they contain the duties of the controller that respectively has obtained data from the data subject himself or obtained data from a source other than the data subject himself.

In addition, the text of the data protection principles of **Article 5(1)(a)** and other special legal provisions within the Regulation contain many more details of the principle of transparency, which are linked to specific legal principles, such as the special transparency requirements in **Article 7** for obtaining consent.

Data Minimisation

This is contained under **Article 5(1)(c)** which argues that data processing must be "*adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed*." Here, the term "*necessary*" denotes the idea of proportionality.

Accountability

This speaks about the data controller being responsible for compliance with the principles listed in sub-article 1. This refers to the accountability mechanism. As noted, a controller is defined under the GDPR as the person or entity that determines the means and the purposes of processing. If a trader is installing a cookie on one's device and through it is tracking the browsing patterns and the person's activity on the device, this data collection is an instance of personal data processing and in such case, the trader is the controller. This is because they are determining the means (the how) and the purposes (the why) of the processing. The how is obviously affected through technological means (in the example given, through the installation of a cookie) and the why can be for various reasons. One reason would be a market strategy to push more targeted ads to consumers to increase sales, i.e. commercial communication which is based on algorithmic calculations of one's interests. In this example, under the GDPR, the trader is responsible for and should be able to demonstrate compliance with the core principles.

Here, the user interface and user journey can be used as a documentation tool to demonstrate that users, during their actions on the social media platform, have read and taken into account data protection information, have freely given their consent, have easily exercised their rights, etc.

Rights of the Data Subject

Articles 15 to **22** establish the data subject's rights with the most important ones being:

- The right to access: **Article 15**
  This means that as a data subject, one has a right to know what data of his is being processed and therefore, the right to ask the controller for access to their own data.

- The right to erasure: **Article 17**
  This means that one has the right to know that data has been erased.

- The right to object: **Article 21**
  This means that the data subject has the right to object at any time to the processing of personal data concerning them which is based on either **Article 6(1)(e)** or **Article 6(1)(f)** on grounds relating to their personal situation. If this arises, the controller shall no longer process personal data unless it demonstrates compelling and legitimate grounds for the processing which overrides the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims. This once again goes back to the notion of the balancing of interests.

  Article 21(1) provides the general notions of the right to object.

  When we spoke about consent, it was noted how a data subject has the right to withdraw their consent and the controller must stop or erase data, unless there exists

another legal ground on which they can process it. However, the GDPR also provides for a means to circumvent the processing of one's data when they object when the legal basis for processing is not consent. This is known as the right to object. In this regard, we note that the data subject has the right to object to their data being used in a specific way, even if the legal basis is not consent. Here, one brings a request to the controller to they stop processing their data.

As per **Article 21(2)**: "*Where personal data is processed for direct marketing purposes, the data subject shall have the right to object at any time to the processing of personal data concerning him or her for such marketing, which includes profiling to the extent that it is related to such direct marketing*."

A practical example is the unsubscribe feature on commercial emails and newsletters. While the companies have a legitimate interest to target an individual with advertising, at law, the individual also has a right to object to this and to request it to stop. This is an offshoot of personal data protection.

Article 21(5) indicates that in the context of information society services, notwithstanding the ePrivacy Directive, the data subject may exercise his right to object by automated means using technical specifications. This relates to the manner in which design is used to ensure data protection. A website interface can be designed in such a way so as to pursue certain values, such as an ethical design. In such a scenario, what is done is through technical specifications on the interface, is certain design elements are included that help people enforce their legal rights. This is the relationship between law and technology where a website is designed and coded in a way that enables you to more easily facilitate the exercise and the realisation of one's legal rights.

The aforementioned relationship between law and code (computer software) can be even more prominently be seen in the following example: In the Criminal Code, accessing child pornography is criminal. However, if there exist videos online, a person is a free agent who can choose not to break the law or to break the law and access such videos. However, when governments are made aware that a website is trading in such content, the police introduce a filter at governmental level. This means that anyone trying to access the content will receive an access denied. This is a technological barrier that is written into the code of the website. Therefore, the law criminalises the action, but a person are a free agent. To circumvent that, through the imposition of a filter on the site by law enforcement, an internet block is created which disregard one's agency. This shows the ability of technology to further the aims of the law but still suffers from limitations of enforcement: there are so many online sites that the Data Protection Agency can only do so much to investigate all of them.

This also can apply to privacy rights. An example of this is the website including an easily accessible 'Do Not Track' button in browsers which sends a signal to the

visited websites which, if they respect the signal, will stop tracking the clicks, searches and reading habits of visitors. This relates greatly to the idea of deceptive design of an interface. It is very interesting to see how technology can be used to protect one's rights as opposed to using solely substantive rights as a means of protection, as the latter often suffer from issue with enforcement.

- Automated individual decision-making, including profiling
  It is sometimes the case that the data controller has so much information that it can make inferences about the data subject. The decision to target the data subject with an advert is an automated one taken by a machine based on an algorithmic computer system, likely AI and not a human who makes such an inference based on previous shopping experiences.

- The right to data portability.

Data Protection by Design and By Default

Here, we take note of a very important article, namely, **Article 25(1)**:

> *Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects.]*

Data protection by design: A website must be designed in a manner to implement data protection principles. If one of the principles is data minimisation, then the website should be designed and programmed only to collect the data which is necessary. We note that a website can be designed in a way that makes it unintuitive for users to either decline cookies or learn more about how their data is being processed and stored or to change data preferences. When websites obscure or make it difficult to find these settings to manage how much data is being shares with the internet service provider, or when a website makes enabling such changes more onerous than necessary, they are infringing this provision of the GDPR which argues that the design of a website must protect data protection. Otherwise, the website is considered to be deceiving, manipulating or coercing its users to giving more data than they want to share. This emphasises the relationship between code (the intentional design of the website) and protection of data.

There are some key elements that controllers and processors have to take into account when implementing data protection by design. One of them is that with regard to the principle

of fairness, the data processing information and options should be provided in an objective and neutral way, avoiding any deceptive or manipulative language or design

Data protection by default: This emphasises the necessity of active, informed consent when it comes to sharing personal data for additional purposes beyond what is essential for a service or contract in online settings where privacy settings may include toggles for users to opt-in or opt-out of data sharing for non-essential purposes. The GDPR mandates that by default, user privacy settings should be configured to not share personal data until the user explicitly opts-in. This approach ensures that individuals have full control over their data and are not automatically subjected to data sharing practices they may not want. By making the default option 'no' for sharing personal data, it encourages users to actively consider and decide whether they want to opt-in for sharing additional data. This requirement serves to protect individuals' data privacy rights by promoting transparency, choice, and active consent in data processing practices. It discourages the use of default settings that automatically enable data sharing, as such practices may lead to individuals inadvertently sharing more data than they intend or are comfortable with. This also inherently links with the manner in which the website is designed.

The Guidelines identify elements of the principles for Data Protection by Default and Data Protection by Design, among other things, which become even more relevant with regard to deceptive design patterns.

- Autonomy: Data subjects should be granted the highest degree of autonomy possible to determine the use made of their personal data, as well as autonomy over the scope and conditions of that use or processing.

- Interaction: Data subjects must be able to communicate and exercise their rights in respect of personal data processed by the controller.

- Expectation: Processing should correspond with data subjects' reasonable expectations.

- Consumer choice: The controllers should not 'lock in' their users in an unfair manner. Whenever a service processing personal data is proprietary, it may create a lock-in to the service, which may not be fair if it impairs the data subjects' possibility to exercise their right of data portability in accordance with **Article 20** of the GDPR.

- Power balance: This should be a key object of the data controller – data subject relationship. Power imbalances should be avoided and when this is not possible, they should be recognised and accounted for with suitable counter measures.

- No deception: Data processing information and options should be provided in an objective and neutral way, avoiding any deceptive or manipulative language or design.

Compliance with Data Protection by Default and Data Protection by Design is important when assessing deceptive design patterns, as it would result in avoiding them in the first place. Indeed, confronting one's service and associated interfaces to the elements comprising Data Protection by Default and by Design principles, such as the ones mentioned above, will help identify aspects of the service that would constitute a deceptive design pattern before launching the service.

ePrivacy Directive – Controlling the Collection and Reuse of Personal Information

This directive was enacted at a time when there was the Data Protection Directive, which today has been replaced by the GDPR. When it was in force, this legislation had the general goal to cover all of data protection. The ePrivacy Directive applies the rules of data protection to a specific sector, i.e. the electronic communications sector. Therefore, in essence, it is a sector specific implementation of data protection laws. Today, the GDPR acts as the most general rule with the ePrivacy Directive simply being the more specific implementation of the principles contained therein to a specific sector. For this reason, many regard it as superfluous.

Nevertheless, it does have a specific provision for the regulation of cookies. In a nutshell, in 2009 through the amendments to this directive, in the EU, any cookies which are not essential (i.e. those cookies are not essential for a website to operate) require the consent of the data subject - the opt-in, positive consent. Essential cookies do not require such consent.

Cookies and Behavioural Targeting

Cookies are frequently used by internet sites. For example, on a website, cookies may be used to identify the fact that a particular machine (and often by inference a particular individual) has access the site previously and thus, it may be useful to customise the page presented according to previous activity the user has engaged in. Typically, an electronic commerce site may present users with a list of recommended buys based on an analysis of that person's purchasing history.

Websites mainly use cookies to:

- Identify users.
- Remember consumer preferences.
- Help users complete tasks without having to re-enter information when browsing from one page to another or when visiting the site later.

Cookies can also be used for online behavioural advertising and to show adverts relevant to things the user searched for in the past. Such practises may be welcomed in many instances. However, there are also implications for the privacy and anonymity of users.

Article 5(3) of the directive provides that:

> *Member States shall ensure that the storing of information or the gaining of access to information already stored in the terminal equipment of a subscriber or user is only allowed on condition that the subscriber or user concerned has given his or her consent having been provided with clear and comprehensive information, in accordance with Directive 95/46/EC, inter alia, about the purposes of the processing. This shall not prevent any technical storage or access for the sole purpose of carrying out the transmission of a communication over an electronic communications network, or as strictly necessary in order for the provider of an information society service explicitly requested by the subscriber or user to provide the service.*

This article first distinguishes between essential and optional cookies and noted that in relation to optional cookies prior informed consent for the storage of or access to information stored on a user's terminal equipment is required since a cookie is installed on a user's device with data being stored on that cookie which is connected to every user every time there is an interaction. Therefore, internet service providers must ask user if they agree to cookies and similar technologies, such as beacons, in order for them to be used. For consent to be valid, as we have seen, it must be informed, specific, freely given and must constitute a real indication of the individual's wishes.

In the context of cookies, there are issues and controversies about how explicitly the level of notification needs to be. A common formulation used by websites owners is along the lines of "*We use cookies to enhance your browsing experience*", which is a rather vague formulation.

Another issue relates to the extent to which a user may legitimately be put into a situation where the choice is between accepting cookies or eschewing access to the website.

With regards to essential cookies, we note that there are exemptions to this need for consent. This exemption only applies if the cookies are:

- Used for the sole purpose of carrying out the transmission of a communication, i.e., session cookies.

- Strictly necessary in order for the provider of an information society service to provide the service explicitly required by the user.

The exceptions to the rule established by **Article 5(3)** are rooted in functional necessities for the basic communication or extra services requested by the subscriber or user and expressed in conformance with the limited retention of data principle.

The amount of data privacy laws protecting individuals when they are online highlight the fact that on the internet, we are constantly being surveyed and tracked, with our personal preferences collected, stored and analysed to target us with advertising us and, in some cases,

manipulate us. These principles and legislation of data protection as well as those under consumer protection law, as shall be seen, are means to resist the negative side of the internet and the negative effects of this form of monitoring. The law attempts to find solutions to these forms of infringements.

In order to best deal with questions of this nature, we must:

1. Undertake a description of the context including whether the situation pertains solely to a data subject and controller or whether the data subject is also dually a consumer bringing in consumer protection law.

2. Identify the relevant legal provisions. Considering only data protection law, we must check **Article 5** including:

    a. Transparency – Controllers or processers must provide the information to users when signing up efficiently and succinctly as to the processing of their personal data. Such must be clearly differentiated from other non-data protection related information and in clear and plain language.

    b. Consent – If consent is the legal basis on which processing is predicated, we look to the definition under **Article 4(11)** to check whether it satisfies the requirements of being "*freely given, specific…*" etc. Here, we must ensure that consent is presented in a manner which is clearly distinguishable from other matters such as the terms and conditions, in clear and accessible language as per **Article 7(2)** of the GDPR. We also must ensure consent was given by a clear affirmative act as per **Recital 32** with the user provided the opportunity to opt in to further data sharing at a later stage through the data protection settings. Here lack of consent should be the default state until consent has been given.

    Additionally, as per **Article 7(3)** we must ensure that users are able to withdraw consent at any time and that they are informed of such from the onset. Controllers shall demonstrate that users have the possibility to refuse providing consent or to withdraw the consent without any detriment. Users of social media platforms who consent to the processing of their personal data with one click, for example, by ticking a box, shall be able to withdraw their consent in an equally easy way. Therefore, consent is a reversible decision which a prerequisite for valid consent to be given.

3. Consider whether there exist any deceptive design patterns to consider and whether they relate to any GDPR provisions.

Consumer Protection Law

When considering consumer protection vis-à-vis online activities, especially in relation to dark patterns, we firstly must highlight the digital consumer-trader relationships and the digital asymmetry that arises therefrom. In such scenarios, the trader has access to the consumer's detailed person profile including decision-making biases and pressure points. At the same time, the trader also controls and shapes the entire environment in which the consumer operates. This creates the aforementioned asymmetry between the two based on the embedded vulnerability of the consumer, preventing them from interacting on an equal footing for many reasons:

- The complexity and power enjoyed by the trader.
- The way the interfaces are designed and operated.
- The fact that the trader benefits from detailed insights about the consumer, while the consumer often knows or understands very little of how the trader and the service operates.

Under conditions of digital asymmetry, all digital consumers are rendered vulnerable and such vulnerability is considered by the relevant legislation when analysing the consumer benchmark in these new market realities. This is why consumer law is so essential as it protects individuals in a B2C context to protect the weaker party in the contractual relationship. This is important to keep in mind as if Person A is contracting with Person B online, where Person B is also a consumer, then Person A isn't afforded any of the benefits under consumer protection law as there isn't a weaker party. This is one of the reaosns why transparency is so essential.

Therefore, while the digital economy has brought about many benefits for consumers, it has also raised concerns as to how choice architecture is designed and presented to consumers. This becomes particularly relevant in relation to online platforms and the increasing prevalence of dark patterns and techniques to push consumers to take certain decisions, especially with the effect of scale increasing the economic incentives to deploy such techniques since consumer behaviour in the online environment translates into considerable benefits to companies.

When taking into consideration dark patterns, we note that such may be data-driven and personalised or implemented on a more general basis, tapping into heuristics and behavioural biases, such as default effects or scarcity biases. While, as noted, there isn't a single way to classify dark patterns, for pure illustrative purposes, we can distinguish between different categories of dark patterns. For example:

1. Dark patterns which make certain decisions more prominent or easier to make.
2. Dark patterns which create a false feeling of urgency or scarcity and a fear of missing out.
3. Dark patterns which shame consumers.

4. Dark patterns which obstruct or confuse consumers, for example, questions with a double negative.
5. Dark patterns which blind consumers, for example, sneaking items into the basket.

Under EU consumer law, these practices would need to be assessed on a case-by-case basis in order to establish whether there has been a breach of specific consumer protection provisions. We note that under this horizonal consumer law acquis, dark patterns can be addressed by the **Unfair Commercial Practices Directive**, the **Consumer Rights Directive** and the **Unfair Terms Directive**.

The Unfair Commercial Practices Directive

The UCPD provides the legal framework regulating business practices affecting consumers' economic interests before, during and after the conclusion of a contract. This refers to **Directive 2005/29** amended by **Directive 2019/2161**. The latter is considered to be the *omnibus* directive and amended many areas of consumer law to ensure such laws could tackle the challenges of the modern digital landscape and be effective in enforcement.

It can be distinguished by its horizontal character (its rules apply to all types of products and services and to all methods of marketing and selling, whether online or offline) and a combination of principle-based restrictions and specific prohibitions for certain practices. The fairness of a commercial practice is tested against a general ban of unfair commercial practices, elaborated with a ban of misleading and aggressive practices and a blacklist of practices that are unfair in every circumstance. Commercial practices which do not affect the consumer's economic interests fall outside the scope of the UCPD.

Its legal basis is **Article 114 TFEU** relating to the internal market as having harmonised consumer protection law across borders helps to facilitate trade. In fact, **Article 1** of the directive outlines its functioning as twofold:

1. To contribute to the proper functioning of the internal market.
2. To achieve a high level of consumer protection.

Therefore, through this broad and harmonised protection, consumers are encouraged to shop online in international markets, thereby enhancing the internal market. The instrument goes as far to say under **Article 4** that Member States shall not restrict the freedom to provide services, nor restrict the free movement of goods for reasons falling within the field approximated by this directive. The dual function of protecting the consumer and eliminated barriers through a harmonisation of law is the main aim.

We further take into consideration the scope under **Article** 3. Any piece of EU legislation must be carefully inspected to determine its material scope, and, moreover, the inquiry is especially sensitive where maximum rules are at stake[3] because the consequence is that

[3] Consider the fact that the UCPD is a measure of maximum harmonization as provided for on page 52.

stricter national measures are not allowed. **Article 3** notes that the directive shall apply to "*unfair business-to-consumer commercial practices, as laid down in **Article 5**, before during and after a commercial transaction in relation to a product*."

The UCPD provides the legal framework regulating business practices affecting consumers' economic interests before, during and after the conclusion of a contract, dealing specifically with unfair practices. **Article 2(d)** defines 'commercial practices' as "*any act, ommision, course of conduct or representation, commercial communication including the advertising and marketing, by a trader, directly connected with the promotion, sale or supply of products to consumers*." Therefore, it doesn't touch practices which harm only cometitors' economic interests or which relate to a transaction between traders.

As stipulated, the core of the regime is contained in **Article 5(1)** which notes:

> *Unfair practices shall be forbidden*.

The question lies in how to achieve a harmonised understanding of 'unfairness'. In the EU, when a directive is passed, there can be one of two forms of harmonisation. Firstly, we consider minimum harmonisation, i.e. a minimum protection must be achieved throughout the Union by virtue of the instrument. Here, Member States are allowed to achieve higher levels of protection, but they must at least reach this baseline limit. The problem is that while there is a floor, meaning all States guarantee the same minimum standards, nonetheless, there may still be discrepancies. Otherwise, there can be maximum harmonisation, whereby the EU sets the standard creating both the floor and the ceiling in terms of harmonisation. Since the UCPD is a measure of maximum harmonisation, Member States are precluded from providing more detail. In this regard, we note that Member States must prohibit all practices which are unfair within the meaning of the directive and allow all those which fall within the material scope of the directive and are not to be seen as unfair.

Therefore, fairness lies at the heart of the UCPD. This doctrine acknowledges that cognitive and economic factors can impair decision-making in certain environments and to determine this, there is the need to test based on an "*average consumer*" commonly presumed to be a "*reasonably well informed and circumspect observer*." Here, this fictional, rational and utility-maximisng agent is presumed to gather information, make decisions in an autonomous manner and is sufficiently knowledgeable to critically assess commercial communication. The average consumer benchmark in the unfair commercial practices law reflects the European Union's emphasis on information obligations and transparency as part of an effective consumer protection regime; however, this is not absolute. There is always a presumption of how an average consumer is expected to behave as a critical player in the market. Apart from the definition of 'average 'consumer' as the benchmark for the assessment of the fairness of commercial practices, the UCPD provides a further test to protect the 'vulnerable' consumer 'whose characteristics make them particularly vulnerable to unfair commercial' practices'. This test is used as a benchmark for assessing the fairness of a

commercial practice when it hinders the economic interests of such consumers. In fact, **Article 5(3)** refers explicitly to 'credulity' as a practice that the trader could reasonably be expected to foresee to distort the economic behaviour of users materially. The term covers groups of consumers who may more readily believe specific claims. The term is neutral and circumstantial, so the effect is to protect members of a group who are for any reason particularly open to being influenced by a specific commercial practice. Any consumer can qualify as a member of this group. **Recital 19** provides a non-exhaustive list of characteristics that make a consumer 'particularly susceptible'. Therefore, a dark pattern designed to take advantage of credulity could see the practice qualify consumers as vulnerable, especially if proven that the user behaviour was foreseeable.

Therefore, when dealing with the UCPD, the first step refers to the prohibition of unfair commercial practices. **Article 5(2)** amplifies and defines the terminology of unfairness. As opposed to the GDPR which mentions the core principles to be taken into consideration and leaves their exact meaning and scope up to interpretation, the UCPD goes further and defines what is to be seen as unfair.

> *A commercial practise shall be unfair if:*
>
> a. *It is contrary to the requirements of professional diligence, and*
>
> b. *It materially distorts or is likely to materially distort the economic behaviour with regard to the product of the average consumer whom it reaches or to whom it is addressed, or of the average member of the group when a commercial practice is directed to a particular group of consumers*.

These two cumulatively applicable ingredients of 'unfairness' are the subject of further amplification under **Article 5(4)** which dictates that:

> *In particular, commercial practices shall be unfair which:*
>
> a. *Are misleading, as set out in **Articles 6** and 7.*
>
> b. *Are aggressive, as set out in **Articles 8** and **9**.*

These provisions set out a degree of detail apt to make more concrete the nature of the control envisaged by the directive as outlined. This strengthens the directive and the notion of unfairness, especially compared to the GDPR where the idea of fairness is not that well developed and is often dependent on other principles such as transparency. These are the broadbands of unfair commercial practices.

Further, **Article 5(5)** stipulates that a list of all those commercial practices which shall in all circumstances be regarded as unfair are listed in the directive under Annex I. Such apply to

all Member States equally without discrimination and may only be amended or altered by modification or revision of the directive. These are much more specific than the distinction between the broad categories of misleading or aggressive unfair practices.

Before moving to analyse the types of unfair practices contained under the UCPD, we note that the new Commission notice on the guidance on the interpretation and application of the UCPD confirms that the directive covers dark patterns and dedicates a section to explain how the relevant provisions of the directive can apply to data-driven B2C commercial practices. The Commission indicates that when dark patterns are applied in the context of B2C commercial relationships, the UCPD can be used to challenge the fairness of such practices, together with other instruments, such as the GDPR.

Misleading Unfair Commercial Practices

Article 6 of the UCPD stipulates:

> *A commercial practice shall be regarded as misleading if it contains false information and is therefore untruthful or in any way, including overall presentation, deceives or is likely to deceive the average consumer, even if the information is factually correct*.

Therefore, here we speak towards overall presentation which deceives or is likely to deceive the average consumer. The emphasis of this provision on the presentation through which the information is provided to consumers is very relevant to dark patterns. This is because in many cases of dark patterns, relevant information is hidden or provided in a way that makes the consumer take a certain decision which, in absence of that specific practice, they otherwise would not have taken. This of course would require a case-by-case assessment taking into consideration the effect of a given practice on consumers. However, we consider it important to make clear that the user interface should be considered as a material element to assess the presentation of information to consumers, as indicated in the Commission notice regarding manipulative practices including visually obscuring important information or promoting a specific option, using trick questions and ambiguous language or deploying default interface settings.

For an acion to fall under **Article 6** it must relate to one or more defined matters, with the net cast wide. The practices considered are as follows:

a. *The existence or nature of the product.*

b. *The main characteristics of the product such as its availability, benefits, risks, execution, composition, accessories, after-sale customer assistance and complaint handling, method and date of manufacture or provision, delivery, fitness for purpose, usage, quantity, specification, geographical or commercial origin or the results to be expected from its use, or the results and material features of tests or checks carried out on the product.*

c. *The extent of the trader's commitments the motives for the commercial practice and the nature of the sales process, any statement or symbol in relation to direct or indirect sponsorship or approval of the trader or the product.*

d. *The price or the manner in which the price is calculated, or the existence of a specific price advantage.*

e. *The need for a service, part, replacement or repair.*

f. *The nature, attributes and rights of the trader or his agent, such as his identity and assets, his qualifications, status, approval, affiliation or connection and ownership of industrial, commercial or intellectual property rights or his awards and distinctions.*

g. *The consumer's rights, including those arising in* ***Directive 1999/44/EC*** *on certain aspects of the sale of consumer goods and associated guarantees.*

As per **Article 6(2)** we also consider that a commercial practice may be misleading if, in its factual context, taking account of all its features and circumstances, it causes or is likely to cause the average consumer to take a transactional decision that he would not have taken otherwise. This must pertain to:

a. *Any marketing of a product, including comparative advertising, which creates confusion with any products, trade marks, trade names or other distinguishing marks of a competitor*.

b. *Non-compliance by the trader with commitments contained in codes of conduct by which the trader has undertaken to be bound, where:*

    i. *The commitment is not aspirational but is firm and capable of being verified, and*

    ii. *The trader indicates in a commercial practice that he is bound by the code.*

c. *Any marketing of a good, in one Member State, as being identical to a good marketed in other Member States, while that good has significantly different composition or characteristics, unless justified by legitimate and objective factors.*

Here, the term 'transactional decision' is defined under the directive as "*any decision taken by a consumer concerning whether, how and on what terms to purchase, make payment,in whole or in part for, retain or dispose of a product or to exercise a contractual right in relation to the product, whether the consumer decides to act or to refrain from acting*."

In a similar way, **Article 7** concerns misleading omissions, i.e. when a "*commercial practice in its factual contexts, taking account of all its features and circumstances and the limitations of the communication medium, omits material information that the average consumer needs, according to the context, to take an informed transactional decision.*" Such therefore causes, or is likely to cause the average consumer to take a transactional decision which otherwise they would not have taken. This can become relevant when it comes to dark patterns used to hide information from consumers to make them take a certain transactional decision. The definition of a misleading ommission is as follows, as per **Article 7(2)**:

> *It shall also be regarded as a misleading omission when, taking account of the matters described in paragraph 1, a trader hides or provides in an unclear, unintelligible, ambiguous or untimely manner such material information as referred to in that paragraph or fails to identify the commercial intent of the commercial practice if not already apparent from the context, and where, in either case, this causes or is likely to cause the average consumer to take a transactional decision that he would not have taken otherwise.*

This can happen, for example, in the context of cost-traps when consumers are induced to believe that a digital service is provided after a one-off payment but later subsequent payments are needed to continuing using the service, as per **Article 7(4)(c)**. In video games, a common issue is that it is made technically possible to continue using the service without paying, but the experience is severely diminished. Another important example could arise if a contracting party fails to outline that they are not a trader which makes a difference seeing as the other party is no longer entitled to consumer rights, as is outlined in **Article 7(4)(f)**.

Aggressive Unfair Commercial Practices

In this regard, we take into accont **Articles 8** and **9**.

According to **Article 8**, a commercial practice "*shall be regarded as aggressive if, in its factual context, taking account of all its fatures and circumstances, by harassment, coercion, including the use of physical force, or undue influence, it significantly impairs or is likely to significantly impair the average consumer's freedom of choice or conduct with regard to the product and thereby cause him or is likely to cause him to take a transactional decision that he would not have taken otherwise*."

This provision is completed by **Article 9** which provides the material elements to take into account when assessing an aggressive practice, including amplifying the notions of harassment, coercion and undue influence. This further includes the exploitation by the trader of any specific misfortune or circumstance of such gravity as to impair the consumer's judgement, of which the trader is aware, to influence the consumer's decision with regard to the product. Many forms of dark patterns can be captured by this provision particularly because the trader, via the techniques used to revamp the user interface (e.g., A/B testing), is

aware of the choices that are most likely to be made by consumers under different circumstances and therefore can use that fact to their own advantage.

> *In determining whether a commercial practice uses harassment, coercion, including the use of physical force, or undue influence, account shall be taken of:*
>
> *a. Its timing, location, nature or persistence.*
>
> *b. The use of threatening or abusive language or behaviour.*
>
> *c. The exploitation by the trader of any specific misfortune or circumstance of such gravity as to impair the consumer's judgement, of which the trader is aware, to influence the consumer's decision with regard to the product.*
>
> *d. Any onerous or disproportionate non-contractual barriers imposed by the trader where a consumer wishes to exercise rights under the contract, including rights to terminate a contract or to switch to another product or another trader.*
>
> *e. Any threat to take any action that cannot legally be taken.*

As outlined previously, through **Article 5(5)**, the UCDP points us towards Annex I which contains certain commercial practices which are in all circumstances considered unfair. These are blacklisted *in toto*. Here, we are looking at the final level of the consideration under the UCPD which is the most precise. Thus, the directive's structure is to apply a general test of unfairness, as outlined in **Article 5(1)**, supplemented by the control of two particular types of unfair practice, the misleading and the aggressive as outlined under **Article 5(4)** – and this is then hardened up still further by the 'black list' in Annex 1, which contains a list of 31 practices that are "*in all circumstances considered unfair.*"

These particular practices are highly relevant to dark patterns, as specific dark patters that amount to unfair commercial practices will be prohibited under the UCPD.

Example 1: Nagging

> This relates to **practice 26** under Annex 1 referring to *"making persistent and unwanted solicitations by telephone, fax, email or other remote media*".
>
> This further relates to **Articles 8** and **9** since it is a form of harassment, including **Article 9(b)**, "*use of threatening or abusive language or behaviour.*"

Example 2: Activity Messages

> Here, we consider **Article 6** which deals with misleading action, in this regard, in relation to availability and quality.
>
> We also consider **practice 7** of Annex 1 referring to "*falsely stating that a product will only be available on particular terms for a limited time*." This pushes consuemrs

to take quick decisions instead of giving them the opportunity to make an informed choice as a form of dark patter.

Further, we regard **practice 18** speaking about "*passing on materially inaccurate information on market conditions or on the possibility of finding the product with the intention of inducing the consumer to acquire the product at conditions less favourable than normal market conditions*."

Example 3: Bait and Switch

Here, we consider **practice 6** on "*making an invitation to purchase a given product with the intion of making the consumer purchase a different one*." Generally speaking where the user interface creates an expectation for the desired item, offered at an attractive price, then discloses its unavailability, substituting it with a different one instead.

Example 4: Testimonials

Here, we outline **practise 23b** which involives "*stating that reviews of a product are submitted by consumers who have actually used or purchased the product without taking reasonable and proportionate steps to check that they originate from such consumers.*"

Additionally, we consider **practice 23c** involving "*submitting or commissioning another legal or natural person to submit false consumer reviews or endorsements, or misrepresenting consumer reviews or social endorsements in order to promote products*.

We further take notice of **Article 7(6)** dealing with misleading omissions. It notes that "*where a trader provides access to consumer reviews of productions, information about whether and how the trader ensures that the published reviews originate from consumers who have actually used or purchased the product shall be regarded as material*."

Example 5: Price Comparison Prevention

Firstly, we consider **Article 6** dealing with misleading actions vis-à-vis overall presentation and comparative advertising.

Secondly, we consider **Article 7** dealing with misleading omissions since price is material information.

It is therefore important that enforcement authorities, when considering breaches to the practices prohibited in the annex of the UCPD, consider whether these practices could be materialised by means of user interface and dark patterns. In this regard, we briefly consider enforcement under **Article 11**. While this directive doesn't exclude the control pursuant to codes of conduct which are defined to mean agreements not imposed by law, i.e. self-

regulation pursuant to standards of trade associations, this must be supplementary to and not a replacement for recourse to proceedings envisaged by **Article 11**.

This article notes that the means to combat undair commercial practices must include legal provisions under which persons or organisations regarded under national law as having a legitimate interest in combating unfair commer- cial practices, including competitors, may: take legal action against such unfair commercial practices; and bring such unfair commercial practices before an administrative authority competent either to decide on complaints or to initiate appropriate legal proceedings. The remedy provided for under the UCPD is for a court or administrative authority to order the cessation, or to institute legal proceedings for an order for the cessation, of unfair commercial practices; or if the unfair commercial practice has not yet been carried out but is imminent, to order the prohibition of, or to institute legal proceedings for an order for the prohibition of, the practice, even without proof of actual loss or damage or intention or negligence on the part of the trader. These remedies are essential in the context of prohibiting or stopping dark patterns which harm or pose a threat of harm to consumers even before any contractual transaction may have been entered into.

The Consumer Rights Directive

The Consumer Rights Directive (CRD) is relevant when discussing dark patterns since it provides for information obligations and information requirements before the conclusion of a contract. The directive indicartes that in distance contracts, the information needs to be provided in a "*way approproate to the means of distance communication used in plain and intelligible language*."

This transparency requirement has been extrapolated from the **Unfair Contract Terms Directive** and requires consumers to be able to understand the information that is being provided and the consequences of entering into a contract. Through the design of the interface, trader can breach this transparency requirement by hiding some material information and deviating consumer's attention to other elements. For example, the trader can include information regarding shipping costs in case of withdrawal from the contract in a separate place while promoting free delivery and giving the impression to consumers that any potential return is also free. The CRD provides more detailed precontractual information requirements than the information requirements in **Article 7(4)** of the UCPD.

The prohibition of **Article 22** on pre-ticked boxes is also relevant since the very essence of the prohibition was to prevent traders from taking advantage of consumers' status quo biases.

Nonetheless, the CRD suffers from many limitations including:

- The aforementioned **Article 22** doesn't apply to sectors excluded from the CRD, such as financial services.

- Similarly, in certain situations, while technically complying with the requirements of **Article 22**, companies can still push consumers to un-tick boxes via a misleading user

interface, for example, by placing the button to go to the next page (e.g., in a booking site) right next to the ticked box or in a very similar shape and colour or by making it look like ticking the box is required in order to proceed. Thus, we consider that it would be important to add also to the CRD an anti-circumvention clause preventing traders from relying on dark patterns to bypass the requirements included in the Directive.

- Additionally, except for the right of withdrawal under **Article 9**, the CRD does not regulate the conditions for contract termination.

The Unfair Contract Terms Directive

As considered, the consumer protection regime envisages transparency and protection against unfairness with the UCTD aiming to address the imbalance between the parties and cotnract terms, which can be due to an aysmmetry of information, expertise or bargaining power with the contract terms. As per **C-110/14**:

> *The weaker position of the consumer vis-à-vis the seller or supplier, which the system of protection implemented by Directive 93/13 is intended to remedy, relates both to the consumer's level of knowledge and to his bargaining power under terms drawn up in advance by the seller or supplier, the content of which the consumer is unable to influence.*

Fairness is the substantive test for the legality of contract terms and the application of this directive is dependent on the formation and existence of a contract. Under **Article 3(1)** "*a contractual term which has not been individually negotiated shall be regarded as unfair if, contrary to the requirement of good faith, it causes a significant imbalance in the parties rights and obligations arising under the contract to the detrient of the consumer*."

In the context of dark patterns, the fact that there necessarily needs to be a contract may limit the applicability of the UCTD as in analysing the website design and consquent consumer behaviour, the availability of any solution under the UCTD will be dependent on the ability to identify a contractual relationship between a trader and a consumer.

Should one be found, however, the unfairness of a contractual term shal be assessed "*considering the nature of the goods or services for which the contract was concluded and by referring, at the time of conclusion of the contract, to all the circumstances attending the conclusion of the contract and to all the other terms of the contract or of another contract on which it is dependent*" as per **Article 4**. Such circumstances would include aspects of website design intended to deceive or manipulate the consumer's behaviour.

It is instructive to note that the UCTD does not require that the consumer to provide monetary consideration for a good or service. Dark patterns typically involve a *'consideration'* that is

not ordinarily monetary but takes the form of sharing personal data to track and profile consumers.

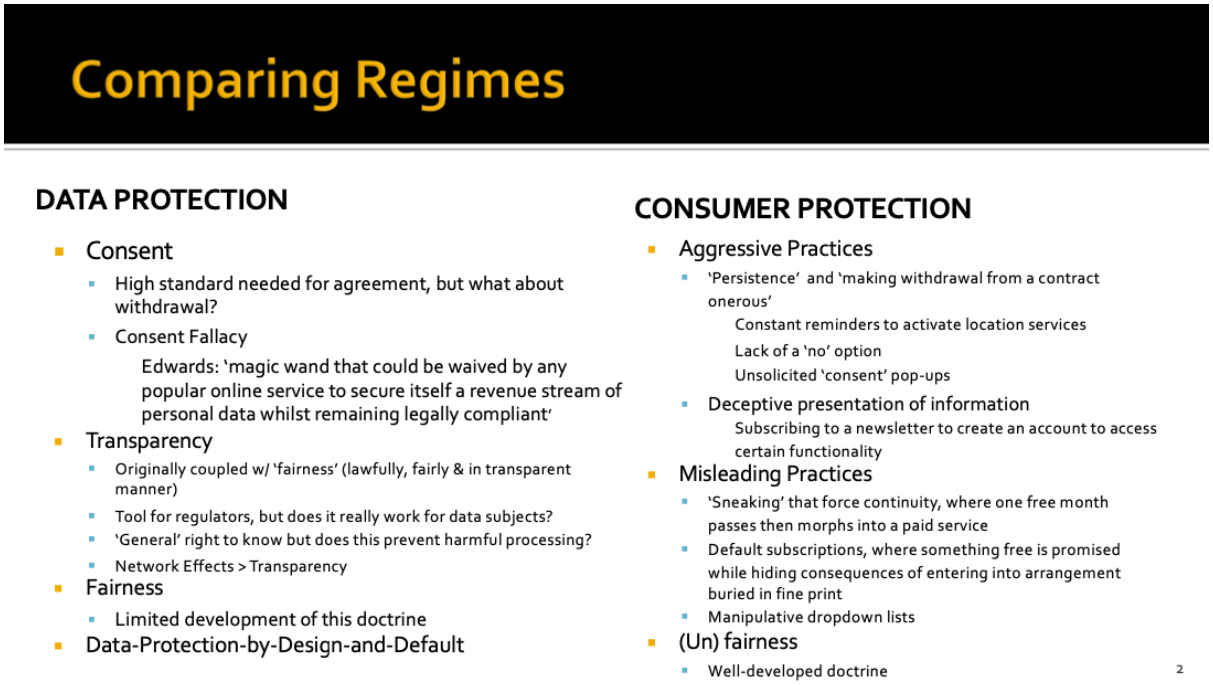
The Electronic Commerce Directive

Regulating Dark Patterns and the Different Legal Regimes in Place

When considering the overarching regimes used to regulate emerging technologies and dark patterns, we consider 'data protection law' and 'consumer protection law'. It is essential to analyse how these overlap and interact with one another in order to find a remedy in the law and to know who to turn to as a regulator.

NB. In Malta, for the enforcement of the GDPR, we turn to the Office of the Information and Data Protection Commissioner and in relation to the consumer regime, we turn to the Malta Competition and Consumer Affairs Authority.

While the first goalpost when dealing with dark patterns and deceptive designs was data protection law, the consumer protection laws still remain very important, despite not having been given as much importance in the past. Consumer protection aims to foster user empowerment. The European Data Protection Supervisor stated: "*EU approaches to data protection… and consumer protection shares common goals, including the promotion of growth, innovation and the welfare of individual consumers*." Thus, we must question to what extent the current EU Consumer Protection acquis including *inter alia* the UCPD, CRD and UCTD is placed to make a substantial and complementary contribution towards the curtailing of dark patterns, acting as an effective deterent against them and sanctioning manipulative design techniques like dark patterns. This is especially in light of the European Commission's 'New Deal for Consumers' which strenthened EU consumer law enforcement mechansims and modernised the EU's consumer protection rules.



Intersections between Data Protection and Consumer Protection

Suppose a data subject (in terms of data protection law) is also a consumer (as defined in consumer protection law). In that case, the European Union offers a 'high level of consumer protection' for their economic activities. Additionally, their data protection and privacy rights are robust seeing as citizens of the EU are said to have a 'strong, comprehensive and enforceable privacy protection framework' flowing from the Charter of Fundamental Rights of the EU as well as through the GDPR and the e-Privacy Directive. Further protection comes from the European Convention on Human Rights and laws of the member states, including national constitutions.

Both consumer and data protection laws aim, at least in part, to protect the autonomy of the natural person. In other instances, autonomy is overridden by the interests of protecting the weaker party in an imbalanced relationship. However, protection as a consumer concept is more tangible. While privacy and data protection law involves a complex balancing of interests in various contexts, consumer protection aims to address power differentials based inter alia on information asymmetries and bargaining power.

We question when is consumer law perhaps most adept to deal with situations and provide a remedy in the case a data-subject is also a consumer?

1. When dealing with mtters pertaining to fairness.
   Fairness is broader in consumer protection than data protection, as outlined. It would be more suitable to hold data controllers to account. The Unfair Commercial Practices Directive will consider a dark pattern unfair if it is "*contrary to the requirements of professional diligence and materially distorts or is likely materially to distort the economic behaviour of the average consumer concerning the product*". In turn, "*to materially distort the economic behaviour of consumers*" is defined as "*using a commercial practice to appreciably impair the 'consumer's ability to make an informed decision, thereby causing the consumer to take a transactional decision that he would not have taken otherwise*". The GDPR is not as detailed and requires other elements to support its understanding of fairness.

2. When dealing with matters pertaining to participation opportunities when seeking a judicial or administrative remedy.
   The GDPR does not require member states to allow complaints by advocacy groups independently of a data subject's mandate; it merely permits them to do so. Conversely, **Article 11(1)** of the Unfair Commercial Practices Directive and **Article 7(2)** of the Unfair Contract Terms Directive requires member states to ensure consumer rights organisations can bring an action before the national courts and administrative authorities.

3. The consumer protection regime provides more opportunities and remedies (i. e., damages, enforcement measures, including discontinued use of unfair terms) than the regime for personal data protection.

NB. It remains unclear whether the supply of personal data to a trader constitutes a contract. A contract remains where "*the trader supplies or undertakes to supply digital conent or a digital service to the consumer and the consumer pays or undertakes to pay a price*". Therefore, one would need to look towards national legal framework to determine whether parties have formed a contract. This legal point is relevant where the application of consumer protection is dependent on the ex- istence of a contract, such as in the Unfair Consumer Terms Directive (UCTD).

An example of overlap between data protection and consumer protection law happens in the following scenario: Person A is a data-subject and a consumer on a social media platform. We consider that the EU consumer protection regime sees personal data as having economic value but without resorting to the bestowment of property rights to data subjects over their data. In fact, the Guidance on the UCPD's application recognises that personal data, consumer preferences and other user-generated content, have a *'de facto'* economic value and are sold to third parties. We note that as per **Aricle 6(1)** of the GDPR, personal data is lawfully processed *inter alia* if consent has been given by the consumer or if the processing is necessary for the performance of the contract or is necessary for the purpose of the legitimate intersts pursued by the data controller. Say, the data controller relies on **Article 6(1)(a)** and the legal basis of consent as a ground for processing, such consent must be obtained prior to the data being processed. Otherwise, we consider that the processing carried out during the period of time from the moment processing started until consent is obtained would be unlawful. Under the UCPR, if a trader fails to disclose, or fails to tell in a clear, intelligible and timely maner that the person data provided by the consumer will be processed and used for the commercial activities of the trader, this would be a misleading omission under **Article 7** and a violation of data protection law. This means both the UCPD and the GDPR can be made use of to seek a remedy.

Under the EU Directives discussed above, there is a general obligation for the Member States to ensure that 'adequate and effective means 'exist' to ensure compliance with the Directives in the interests of consumers. Collectively, the Consumer Rights Directive, the Unfair Contract Terms Directive, and the Unfair Commercial Practices Directive could play a substantial part in regulating dark patterns. However, applying consumer protection law without increasing the ability to enforce the regime will only lead to frustration and disappointment.

The consumer protection legislation of the EU can stand on its own as a powerful enfrocer against dark patterns. By purposely moving away from terms commonly found in the design literature to describe dark patterns, this article has put these and other techniques into the language of consumer protection regulators. The analysis reveals that, when used appropriately, this regime could have significant potential in restraining the deployment of

manipulative design features that affect users across the pre-contractual, contractual, and post-contractual environments found embedded in user inter- faces and system architectures.

In some cases, the proscription of the dark pattern will be clear cut; others will require further development of the law. Some will need creative interpretations by regulators to stop the abusive practice. With enhanced harmonization and a new right to individual remedies when unfair commercial practices harm, alongside enhanced protection of consumers using 'free' digital services, the consumer protection regime will remove its reputational shackles as 'ineffective' and be- come an important enforcer against the use of abusive dark patterns. Fortunately, the flexibility in adopting specific addi- tional measures to respond to 'rapid technological develop- ments concerning online 'marketplaces' is likely to be written into the modernisation of the consumer protection rules.

EU Legislation that may address select Dark Patterns

Example 6: Hard to Cancel/Roach Motel

We first consider **Article 8** UCPD dealing with aggressive practices in the form of coercion, including **Article 9(d)** which speaks of "*imposing onerous or disproportionate non-contractual barriers where a consumer wishes to exercise rights under the contract, including rights to terminate a contract or to switch to another product or another trader*."

Further, there is **Article 7** of the UCPD as a misleading omission pertaining to the right to withdrawal.

We take cognisance of **Article 6(1)(h)** of the CRD dealing with the right to withdrawal, as well as **Articles 10, 14(2)** and **(4)** on consequences.

UCTD Annex point **1(h)** which considers "*Automatically extending a contract of fixed duration where the consumer does not indicate otherwise, when the deadline fixed for the consumer to express this desire not to extend the contract is unreasonably early*"and point **1(i)** dealing with "*irrevocably binding the consumer to terms with which he had no real opportunity of becoming acquainted before the conclusion of the contract*".

Example 7: Intermediate Currency

Initially, we take into account **Article 6** UCPD on misleading action vis-à-vis price and the main characteristic.

Secondly, we consider **Article 7** UCPD on misleading omissions, once again vis-à-vis price and the main characteristic.

Thirdly, we note **Articles 8** and **9** UCPD as a result of aggressive practices due to undue influence, in particular in case of vulnerable consumers, such as young people.

Fourthly, we regard **Article 6(1)(e)** which considers price as a main characteristic.

Example 8: Sneak into Basket

There exists **practice 29** of Annex 1 of the UCPD in this regard which refers to "*demanding immediate or deferred payment for the return or safekeeping of products supplied by the trader, but not solicited by the consumer*."

Further, we take into consideration **Article 27** CRD which speaks of *"inertia selling consequences – consumers exempted from the obligation to provide consideration for unsolicited products*." In this regard, the absence of a response from the consumer is not consent.

Example 9: Hidden Costs

Firstly, we consider both **Article 6** and **7** of the UCPD dealing with misleading action and omission respectively in relation to price.

The question of price also brings in the application of **Article 6(1)(e)**.

Other than that, we consider **Article 22** of the CRD which notes that the "*trader needs the consumers' express consent for any payment in addition to the remuneration agreed upon for the trader's main contractual obligation*."

Finally, we take note of the UCTD and **Article 4(2)** and **Article 5** which requires the communication to be made in "*plain intelligible language*". Therefore, the consumer must be put in a position to clearly understand the economic consequences stemming from the contract.

Example 10: Hidden Subscription/False Continuity

Initially, we note misleading action and omission under **Articles 6** and **7** of the UCPD. In relation to the former we consider the main characteristics and price and in relation to the latter we outline hiding, ambiguity on main characteristics, price, right of withdrawal and cancellation.

Then, we take into account coercion bringing about the application of **Articles 8** and **9** of the UCPD**.**

Further, we regard **Article 6** of the CRD dealing with price, main characteristics and right of withdrawal. This also brings to the fore **Article 8(2)** which deals with information being provided in a clear and prominent manner.

Finally, we take into account the UCTD and Annex **1(h)** which "*automatically extends a contract of fixed duration where the consumer does not indicate otherwise, when the deadline fixed for the consumer to express this desire not to extend the contract is unreasonably early.*"

Example 11: Hidden Information/False Hierarchy

We keep in mind **Article 6** of the UCPD on misleading action which in this case pertains to characteristics, price, consumers' rights and the overall presentation of information.

Secondly, we take into account **Article 7** of the UCPD dealing with misleading omissions vis-à-vis hiding, making information unclear, ambiguous and untimely.

Thirdly, we regard **Article 6** of the CRD and **Article 8(2)** which deals with information being provided in a clear and prominent manner.

Finally, the GDPR comes into play in relation to the data protection principles, in particular of transparency and fairness, as well as **Article 25** dealing with data protection by design and default.

Example 12: Preselection (Default)

We keep in mind **Article 6** of the UCPD on misleading action which in this case pertains to the need of a service.

We also take into account **Article 8** in relation to aggressive practices, in this case, coercion and undue influence.

Article 22 of the CRD plays a role as it calls for express consent of a consumer for additional charges and stipualtes that such cannot be inteferred.

We also take into consideration the GDPR, namely **Article 25** on data protection by design and default, the data protection principles under **Article 5(1)** and also **Article 4(11)** and **Article 7** on conditions of consent. In this particular scenario, we are reminded that as per **C-673/17)**, pre-ticked boxes don't constitute valid consent under the GDPR.

Name of dark pattern	Relevant legislation
Nagging	UCPD Annex 1 Practice 26 (Making persistent and unwanted solicitations by telephone, fax, e-mail or other remote media) UCPD Art. 8-9 Aggressive practice (harassment), including Art. 9(b) (use of threatening or abusive language or behaviour) DMA (anti-circumvention rule)
Activity messages	UCPD Art. 6 Misleading action (availability, quantity) UCPD Annex 1 Practices 7 (Falsely stating that a product will only be available for a very limited time, or that it will only be available on particular terms for a very limited time, in order to elicit an immediate decision and deprive consumers of sufficient opportunity or time to make an informed choice) and 18 (Passing on materially inaccurate information on market conditions or on the possibility of finding the product with the intention of inducing the consumer to acquire the product at conditions less favourable than normal market conditions)
Testimonials	UCPD Annex 1 Practices 23b (Stating that reviews of a product are submitted by consumers who have actually used or purchased the product without taking reasonable and proportionate steps to check that they originate from such consumers) and 23c (Submitting or commissioning another legal or natural person to submit false consumer reviews or endorsements, or misrepresenting consumer reviews or social endorsements, in order to promote products) UCPD Art. 7(6) Misleading omission (Where a trader provides access to consumer reviews of products, information about whether and how the trader ensures that the published reviews originate from consumers who have actually used or purchased the product shall be regarded as material)
Hard to cancel / roach motel	UCPD Art. 8 Aggressive practice (coercion), including Art. 9(d) (impose onerous or disproportionate non-contractual barriers where a consumer wishes to exercise rights under the contract, including rights to terminate a contract or to switch to another product or another trader) UCPD Art. 7 Misleading omission (right of withdrawal) CRD Art. 6(1)(h) (right of withdrawal), Art. 10 and Art. 14(2), (4) (consequences) UCTD Annex point 1(h) (Automatically extending a contract of fixed duration where the consumer does not indicate otherwise, when the deadline fixed for the consumer to express this desire not to extend the contract is unreasonably early) and point 1(i) (Irrevocably binding the consumer to terms with which he had no real opportunity of becoming acquainted before the conclusion of the contract) DMA (anti-circumvention rule)
Price comparison prevention	UCPD Art. 6 Misleading action (overall presentation, comparative advertising) UCPD Art. 7 Misleading omission (price as material information)
Intermediate currency	UCPD Art. 6 Misleading action (price, main characteristics) UCPD Art. 7 Misleading omission (price, main characteristics) UCPD Art. 8-9 Aggressive practice (undue influence, in particular in case of vulnerable consumers such as young people) CRD Art. 6(1)(e) (price, main characteristics)

Sneak into basket	UCPD Annex 1 Practice 29 (Demanding immediate or deferred payment for or the return or safekeeping of products supplied by the trader, but not solicited by the consumer) CRD Art. 27 (inertia selling consequences - consumers exempted from the obligation to provide consideration for unsolicited products; absence of a response from the consumer is not consent)
Hidden costs	UCPD Art. 6 Misleading action (price) UCPD Art. 7 Misleading omission (price, hiding or providing in an untimely manner) CRD Art. 6(1)(e) (price) CRD Art. 22 (trader need the consumers' express consent for any extra payment in addition to the remuneration agreed upon for the trader's main contractual obligation) UCTD Art. 4(2), Art. 5 (plain intelligible language; consumer must be put in a position to clearly understand the economic consequences stemming from the contract (e.g. Case C-609/19))
Hidden subscription / forced continuity	UCPD Art. 7 Misleading omission (hiding, ambiguity on main characteristics, price, right of withdrawal and cancellation) UCPD Art. 6 Misleading action (main characteristics, price) UCPD Art. 8-9 Aggressive practice (coercion) CRD Art. 6 (price, main characteristics, right of withdrawal), Art. 8(2) (information must be provided in a clear and prominent manner before placing the order) UCTD Annex 1h (Automatically extending a contract of fixed duration where the consumer does not indicate otherwise, when the deadline fixed for the consumer to express this desire not to extend the contract is unreasonably early)
Bait and switch	UCPD Art. 6 Misleading action (existence and characteristics of the product) UCPD Art. 7 Misleading omission (hiding, untimely information) UCPD Annex 1 Practice 5 (Making an invitation to purchase products at a specified price without disclosing the existence of any reasonable grounds the trader may have for believing that he will not be able to offer for supply or to procure another trader to supply, those products or equivalent products at that price for a period that is, and in quantities that are, reasonable having regard to the product, the scale of advertising of the product and the price offered) UCPD Annex 1 Practice 6 (Making an invitation to purchase products at a specified price and then: (a) refusing to show the advertised item to consumers; or (b) refusing to take orders for it or deliver it within a reasonable time; or (c) demonstrating a defective sample of it, with the intention of promoting a different product)
Hidden information / False hierarchy	UCPD Art. 6 Misleading action (characteristics, price, consumers' rights, overall presentation of information) UCPD Art. 7 Misleading omissions (hiding, unclear, ambiguous, untimely) CRD Art. 6, Art. 8 (pre-contractual information must be clear and comprehensible) GDPR Art. 5(1) data protection principles, in particular of transparency, fairness, Art. 25 data protection by design and default DMA (anti-circumvention rule)
Preselection (default)	UCPD Art. 6 Misleading action (the need of a service) UCPD Art. 8 Aggressive practice (coercion, undue influence) CRD Art. 22 (express consent of a consumer for additional charges cannot be inferred by using default options) GDPR Art. 5(1) data protection principles, in particular of transparency, fairness, Art. 25 data protection by design and default, depending on circumstances also Art. 4(11) and Art. 7 conditions of consent (pre-ticked boxes do not constitute valid consent under the GDPR - C-673/17) DMA (anti-circumvention rule)
Toying with emotion	UCPD Art. 6 Misleading action (characteristics, benefits and risks of product) UCPD Art. 8-9 Aggressive practice (coercion, undue influence), including Art. 9(b) (Use of threatening or abusive language or behaviour) and Art. 9(c) (Exploitation by the trader of any specific misfortune or circumstance of such gravity as to impair the consumer's judgement, of which the trader is aware, to influence the consumer's decision with regard to the product) UCPD Annex 1 Practices 28 (Including in an advertisement a direct exhortation to children to buy advertised products or persuade their parents or other adults to buy advertised products for them) and 30 (Explicitly informing a consumer that if he does not buy the product or service, the trader's job or livelihood will be in jeopardy) GDPR Art. 5(1) data protection principles, in particular of transparency, fairness, Art. 25 data protection by design and default AVMSD Art. 9(1)(b) (bans subliminal techniques), 9(1)(g) (bans manipulation of minors)
Trick questions	UCPD Art. 6 Misleading action (existence and characteristics of product) UCPD Art. 7 Misleading omissions (unintelligible, ambiguous information) UCTD Art. 4(2) and Art. 5 (contract terms must be in plain and intelligible language) GDPR Art. 5(1) data protection principles, including of transparency, fairness, Art. 25 data protection by design and default DMA (anti-circumvention rule)
Disguised ad	UCPD Art. 6 Misleading action (marketing) UCPD Art. 7(2) Misleading omission (failure to disclose commercial intent) UCPD Annex 1 Practices 11 (Using editorial content in the media to promote a product where a trader has paid for the promotion without making that clear in the content or by images or sounds clearly identifiable by the consumer) and 11a (Providing search results in response to a consumer's online search query without clearly disclosing any paid advertisement or paym specifically for achieving higher ranking of products within the search results) and Practice 28 (Including in an advertisement a direct exhortation to children to buy advertised products or persuade their parents or other adults to buy advertised products for them) UCPD Art. 8-9 Aggressive practice (undue influence) UCPD, AVMSD, eCommerce Directive, DSA (advertisement and commercial communications must be clearly recognised) ePrivacy Directive Art. 13 (unsolicited communications)
Confirmshaming	UCPD Art. 6 Misleading action (need for a service, results to be expected) UCPD Art. 8-9 Aggressive practice (undue influence), including Art. 9(b) (Use of threatening or abusive language or behaviour) and Art. 9(d) (Any onerous or disproportionate non-contractual barriers imposed by the trader where a consumer wishes to exercise rights under the contract, including rights to terminate a contract or to switch to another product or anothe trader)
Forced registration	UCPD Art. 8 Aggressive practice (coercion) UCPD Annex 1 Practice 24 offline scenario applied to the digital environment (Creating the impression that the consumer cannot leave the premises until a contract is formed) UCTD Annex 1i (Irrevocably binding the consumer to terms with which he had no real opportunity of becoming acquainted before the conclusion of the contract) GDPR Art. 5(1) data protection principles, including of transparency, fairness, Art. 25 data protection by design and default
Low stock / high demand message	UCPD Art. 6 Misleading action (availability, quantity) UCPD Art. 7 Misleading omission (hiding information) UCPD Annex 1 Practices 7 (Falsely stating that a product will only be available for a very limited time, or that it will only be available on particular terms for a very limited time, in order to elicit an immediate decision and deprive consumers of sufficient opportunity or time to make an informed choice) and 18 (Passing on materially inaccurate information on market condition or on the possibility of finding the product with the intention of inducing the consumer to acquire the product at conditions less favourable than normal market conditions)
Countdown timer / Limited time message	UCPD Art. 6 Misleading action (availability, quantity) UCPD Art. 7 Misleading omission (hiding information) UCPD Annex 1 Practices 7 (Falsely stating that a product will only be available for a very limited time, or that it will only be available on particular terms for a very limited time, in order to elicit an immediate decision and deprive consumers of sufficient opportunity or time to make an informed choice) and 18 (Passing on materially inaccurate information on market condition or on the possibility of finding the product with the intention of inducing the consumer to acquire the product at conditions less favourable than normal market conditions)
Infinite scroll	Depends on the context of its use and specific circumstances, possibly in breach of UCPD Art 6-7 Misleading practices and Art. 8-9 Aggressive practice (undue influence)
Autoplay	Depends on the context of its use and specific circumstances, possibly in breach of UCPD Art 6-7 Misleading practices and Art. 8-9 Aggressive practice (coercion)

Immortal account	UCPD Art. 7 Misleading omission (hiding, ambiguity on main characteristics, right of withdrawal and cancellation) UCPD Art. 6 Misleading action (main characteristics) UCPD Art. 8-9 Aggressive practice (coercion) CRD Art. 6 (main characteristics, right of withdrawal) GDPR Art. 17 (right to erasure)
Misleading referencing pricing	UCPD Art. 6 Misleading action (existence and characteristics of a product, price, overall presentation) UCPD Art. 7 Misleading omission (hiding, untimely information)
Friend spam	UCPD Art. 6 Misleading action (the motives for the commercial practice, need for a service) GDPR Art. 5(1) data protection principles, including of transparency, depending on circumstances Art. 4(11) and Art. 7 conditions of valid consent for the collection and processing of data ePrivacy Directive Art. 13 (unsolicited communications)
Loot boxes	UCPD Art. 6 Misleading action (main characteristics, price) UCPD Art. 7 Misleading omission (main characteristics, price) UCPD Art. 8-9 Aggressive practice (undue influence, in particular in case of vulnerable consumers such as young people) CRD Art. 6(1) (main characteristics, price, the manner in which the price is to be calculated)

Liability of Online Marketplaces under the Unfair Commercial Practices Directive, the Electronic Commerce Directive and the Digital Services Act

Here, we shall be considering the liability of online marketplaces for breaches of the law. Consumers increasingly shop through online marketplaces like Amazon. For consumers, online marketplaces provide considerable conve- nience: consumers can shop through one trusted channel, having access to a large amount of products from different sellers. For sellers, online marketplaces provide an easy way to reach large populations of potential buyers, while relying on the IT infrastructure of the platform. As a consequence, these platforms have come to play a central role in the marketing of products to consumers

To assess the liability of online marketplaces for breaches of the law, it is essential to understand the dynamics of these platforms. Online marketplaces, such as Amazon, not only market and sell their own products but also provide a platform for third-party sellers to advertise, market, and sell their goods. Consequently, liability can arise from the platform's own conduct as a business or from breaches committed by third-party sellers. In this regard their dual role as a retailer and a platform for third-party sellers makes them central to ensuring compliance with legal standards and safeguarding consumer rights.

The case law of the CJEU has focused on breaches of consumer protection law under the UCPD and on infringements of trademark laws. For the former, it is crucial to consider to what extent online marketplaces are liable when a product is marketed in a way that infringes the UCPD which is meant to protect consumers against unfair marketing. It is often difficult to determine whether and to what extent online marketplaces can be held liable under EU consumer law. One reason why this is difficult is that each consumer law directive paints its own picture in terms of the liability of online intermediaries. Another complication is that online marketplaces – at least under certain conditions – are exempted from liability under the Electronic Commerce Directive and now under the Digital Services Act. This raises the question whether and to what extent this exemption impacts potential liability on the basis of EU consumer law.

Regarding trademark infringements, the seminal cases of **L'Oreal v. eBay (C-324/09)** and **Louboutin v. Amazon (C-148/21)/(C-184/21)** are particularly relevant. These cases examined the extent to which an online marketplace can be held liable for breaches of trademark law by third-party sellers and the platform's responsibility towards its consumers. The judgments highlighted that, *inter alia*, for trademark protection, it is more effective to take action against the online marketplace rather than the individual third-party seller. This is because the marketplace has more influence and resources to address and rectify such issues, however, as we shall be seen, the marketplace cannot invariably be held responsible for the conduct of third-party sellers on the platform.

Exempions of Liability under the Electronic Commerce Directive

Here, we turn to consider **Articles 12** to **15** of the Electronic Commerce Directive which deals with liability of intermediary services providers and the exemptions thereof, introducing a harmonised regime throughout the European Union. The idea behind the liability exemptions in this Directive is that online intermediaries should not be held liable for hosted content if they do not control that content. This should promote the free flow of information on the internet.

In this regard, we define service providers as per **Article 2(b)** of the ECD as: "*any natural or legal person providing an information society service*".

Further, information society services are defined under **Article 1(2)** of **Directive 98/34/EC**, as amended by **Directive 98/48/EC**, as "*any service normally provided for remuneration at a distance, by electronic means and at the individual request of a recipient of services*."

Finally, recipient of a service is defined as "*any natural or legal person who…uses an information society service*."

It is important to note, however, that technically, these provisions are no longer effective and liability of online intermediaries is now dealt with under the Digital Services Act (DSA), specifically under **Articles 4, 5, 6** and **8**, which has been in force since February 2024. The reason that we still discuss these provisions is that the DSA is not a break with the past but simply carries the same regime forward, but modernised to deal with more specific issues. One of the pertinent questions here will ultimately be what the impact of the DSA has been on the potential liability of online market places on the basis of EU consumer law. Nevertheless, since there is no case law interpreteing the DSA, we analyse the provisions of the Electronic Commerce Directive since the manner in which **Article 14** is interpreted is still relevant to **Article 6** of the DSA since the langauge is replicated.

When considering the approach of intermediary service providers to liability, considering that online marketplaces are a form of intermediary service providers, we note that the ECD puts forward a horizontal appraoch, with the various activities that are tantamount to acting as an intermediate service provider tackled separately.

Article 12 discusses "*mere conduits*". We consider this mainly in the context of to an internet service provider and using their service to access illegal content, such as an unauthorised movie. The question arises: is the internet provider liable for my actions since I used their service to access illegal content and engage in illegal activity? We notes that:

> *Where an information society service is provided that consists of the transmission in a communication network of information provided by a recipient of the service, or the provision of access to a communication network, Member States shall ensure that the*

service provider is not liable for the information transmitted, on condition that the provider:

a. *Does not initiate the transmission.*

b. *Does not select the receiver of the transmission.*

c. *Does not select or modify the information contained in the transmission.*

The acts of transmission and of provision of access referred to in paragraph 1 include the automatic, intermediate and transient storage of the information transmitted in so far as this takes place for the sole purpose of carrying out the transmission in the communication network, and provided that the information is not stored for any period longer than is reasonably necessary for the transmission.

This Article shall not affect the possibility for a court or administrative authority, in accordance with Member States' legal systems, of requiring the service provider to terminate or prevent an infringement.

Article 13 deals with caching:

Where an information society service is provided that consists of the transmission in a communication network of information provided by a recipient of the service, Member States shall ensure that the service provider is not liable for the automatic, intermediate and temporary storage of that information, performed for the sole purpose of making more efficient the information's onward transmission to other recipients of the service upon their request, on condition that:

a. *The provider does not modify the information;*

b. *The provider complies with conditions on access to the information;*

c. *The provider complies with rules regarding the updating of the information, specified in a manner widely recognised and used by industry;*

d. *The provider does not interfere with the lawful use of technology, widely recognised and used by industry, to obtain data on the use of the information; and*

e. *The provider acts expeditiously to remove or to disable access to the information it has stored upon obtaining actual knowledge of the fact that the information at the initial source of the transmission has been removed from the network, or access to it has been disabled, or that a court or an administrative authority has ordered such removal or disablement.*

This Article shall not affect the possibility for a court or administrative authority, in accordance with Member States' legal systems, of requiring the service provider to terminate or prevent an infringement.

What is most important for our purposes is **Article 14** and **Article 15**. The former pertains to hosting which is what online marketplace platforms do – they host information. They are essentially an information society service consisting of the storage of information provided by the receipient of the service. We shall focus on these marketplace platforms as a subset of service providers in this regard.

The latter outlines the fact that there is no general obligation to monitor the hosting platform, i.e. EU Member states are precluded from imposing any general monitoring requirements, especially a general obligation to actvely seek facts or circumstances indicating illegal activity. This has generally been taken to mean that these platforms cannot be instructed to proactively look through and filter out illegal content on an ongoing basis, since this would run through the '*notice and take down'* limited liability paradigm. **Recital** 48, however, provides that it is still possible for Member States to require platforms "*to apply duties of care, which can reasonably be expected from them and which are specified by national law, in order to detect and prevent certain types of illegal activity.*"

Where an information society service is provided that consists of the storage of information provided by a recipient of the service, Member States shall ensure that the service provider is not liable for the information stored at the request of a recipient of the service, on condition that:

a. *The provider does not have actual knowledge of illegal activity or information and, as regards claims for damages, is not aware of facts or circumstances from which the illegal activity or information is apparent; or*

b. *The provider, upon obtaining such knowledge or awareness, acts expeditiously to remove or to disable access to the information.*

Paragraph 1 shall not apply when the recipient of the service is acting under the authority or the control of the provider.

This Article shall not affect the possibility for a court or administrative authority, in accordance with Member States' legal systems, of requiring the service provider to terminate or prevent an infringement, nor does it affect the possibility for Member States of establishing procedures governing the removal or disabling of access to information.

Member States shall not impose a general obligation on providers, when providing the services covered by Articles 12, 13 and 14, to monitor the information which they

transmit or store, nor a general obligation actively to seek facts or circumstances indicating illegal activity.

Member States may establish obligations for information society service providers promptly to inform the competent public authorities of alleged illegal activities undertaken or information provided by recipients of their service or obligations to communicate to the competent authorities, at their request, information enabling the identification of recipients of their service with whom they have storage agreements.

Article 14 outlines a general exemption from liability which can be invoked by online intermediary service providers against all sorts of liability claims. This pertains to the '*notice and take down*' limited liability paradigm, a horizonal rule whereby an intermediary becomes liable if they had knowledge or awareness of the illegal activity or content.

Otherwise Member States must ensure that the provider of the hosting service is not liable for the information stored at the request of a recipient of the service, provided that the hosting service provider either does not have actual knowledge of illegal activity or information and, as regards claims for damages, is not aware of facts or circumstances from which the illegal activity or information is apparent; or upon obtaining such knowledge or awareness, acts expeditiously to remove or disable access to the information. Should they not act to "*expeditiously remove or disable access to the information*" once they gain such knowledge or awareness thereof they are able to incur liability.

When speaking about hosting platforms, and liability we distinguish between criminal liability and civil liability. Platforms are exempt from criminal liability in repsect of the storage of information provided by a receipient of their services so long as hey have no actual knowledge of the illegal activity of the information. Further, they are immune from civil liability as long as they have no knowledge of the infringement and are not aware of the facts and circumstances from which the illegal activity or information is apparent.

In this regard, we consider that the underlying liability is not actually mentioned and can come from any law making content illegal including defamation law, trademark law, intellectual property law, consumer law etc.

More specific guidance in relation to online marketplaces was presented by the CJEU in 2011 in **L'Oréal v. eBay (C-324/09)** to better understand how the liability excemptions under Article 14 pertained to online marketplaces like eBay. This case concerned the infringement of intellectual property rights via a platform (in this case: eBay). The CJEU stresses that:

> *…the mere fact that the operator of an online market- place stores offers for sale on its server, sets the terms of its service, is remunerated for that service and provides general information to its customers cannot have the effect of denying it the exemptions from liability provided for by Directive 2000/31.*

Hence, online marketplaces are not as such excluded from applicability of the liability exemption. At the same time, the CJEU does stress that the liability exemption of **Article 14** Directive applies only to the operator of an online marketplace "*if that operator has not played an active role allowing it to have knowledge or control of the data stored*". The CJEU specifies that an operator of an online marketplace does play an active role (and thus is not entitled to rely on the liability exemption) if the operator "*provides assistance which entails, in particular, optimising the presentation of the offers for sale in question or promoting them*." Whether this is the case must be assessed on a case-by-case basis however, liability hinges on this notion of playing an active role.

We consider that the precise understanding of what constitutes an active role remains fairly uncelar till today and when judges in national courts apply this to the facts of the case before them, there is the possibility that they lack clarity and discrepancies are created between judgements, despite the CJEU's attempt to give them an autonomous interpretation. We can't even turn to the ECD or the DSA for clarity as this term is not found within.

Hence, the CJEU does not rule out that online marketplaces can rely on the liability exemption, but as soon as the platform takes an active role in helping to promote the products, it loses the possibility to do so. Therefore, the safe harbour provided by **Article 14** is activity-based. In other words, a company may be exempted from liability in relation to some services but may be found liable for others when the platform is aware of the facts and circumstances from which the illegal activity or information is apparent or it has played an active role, as shall be discussed. For example, if the online marketplace highlights a misleading discount offer on its homepage, the platform is most likely not exempted from liability – even if it was not aware (or should have been aware) that the offer was deceptive. Arguably, optimising the presentation of the sale should be understood to include automized optimalisation. For example, if a platform is giving certain traders a higher ranking in the search results on the platform on the basis of additional payment by those traders, the online marketplace could be seen as optimising the presentation of the offers and, as a consequence, is playing an active role in relation to such offers. In addition, one should keep in mind that optimising an offer is not the only way in which an online intermediary can play an active role. For example, it can be argued that an online marketplace cannot invoke the liability exemption under **Article 14** if it is actively involved in the performance of the sales contract, e.g. when it takes care of the delivery (as Amazon does under the "Fulfillment by Amazon" program). However, the CJEU case law is not conclusive on this matter, leaving considerable uncertainty as to the degree to which online marketplaces can invoke **Article 14** of the E-commerce Directive.

Therefore, under what circumstances would eBay be liable for a breach of trademark law when the original offender is actually a seller? eBay would be liable when they are aware of facts and circumstnaces from which the illegal actvitity or information is apparent.

General Monitoring Obligations

While, as noted under **Article 15** there exists a no general monitoring obligation imposed on Member States, for an online platform to maintain immunity, they must take down any illegal content or information on their platform. We question to what extent can courts issue an injunction on eBay to ensure that counterfeit products are removed? The law exempts platforms from the obligation of general monitoring, recognising that monitoring all activity is impractical. Imposing a publisher model on internet platforms is unfeasible, which is why there is a limited form of immunity from liability.

It is not possible for a court to issue an injunction ensuring that no illegal activity ever occurs on the platform. Instead, the notice-and-take-down approach applies: platforms become liable only when they have knowledge or awareness of illegal content. Once informed, they must act to remove the content, aligning with the limited liability paradigm.

In relation to the '*notice and take down'* liability paradigm, we consider that an intermediary service provider may become aware of illegal content or activity in many different ways, including:

1. By receiving a court order. If an online marketplace receives a court order informing them that there is illegal activity on their platform, they must take steps to remove it.

2. Through notice. If a trademark owner sends information to the platform to note that there are counterfeit products being sold, or there is other illegal activity happen related to their products, the platform is deemed to have become aware and they must expeditiously take it down in order to maintain immunity. Same applies if one receives information from a consumer.

   Here, the issue arises as to what happens if the notice isn't accurate. Although notice can be given, inaccuracies in such notices present a significant problem. This system can result in a form of censorship. For instance, if a user reports a comment on a social network as defamatory, the platform might remove it to avoid liability, even if the comment is not defamatory. This could violate free speech rights.

   The Digital Services Act (DSA) addresses this issue. Procedures that were previously optional are now established by the DSA. The regulation of removing information is governed by the DSA through specific procedures. To give notice, certain conditions must be met, ensuring fair procedure and due process. For example, if a comment on Facebook is reported as defamatory and Facebook removes it to avoid liability, this could infringe on free speech rights if the comment is not actually defamatory. The DSA aims to balance the need to remove illegal content with the protection of free speech by requiring fair and due procedures.

3. Through DSA's own-voluntary initiative investigation and legal compliance provision under **Article 7**, entitled the 'Good Samaritan Clause'. Here, we consider that while

online marketplaces are not obligated to engage in general monitoring, many strive to provide a safe e-commerce environment for their clients. Therefore, it could be that a responsible online marketplace undertakes some level of monitoring to ensure a safe and trustworthy environment. However, this proactive approach can backfire, as voluntary initiatives might lead a court to conclude that the platform should have been aware of any illegal activities.

The ECD recognises the concern that voluntary monitoring could increase liability since monitoring can never be perfect or fully comprehensive. To address this issue, **Article 7** of the DSA provides clarity. It ensures that companies engaging in voluntary monitoring will not lose their immunity solely because of their proactive measures. This provision is a response to the concerns outlined in the ECD, intending to provide peace of mind to platforms that take steps to enhance the safety and reliability of their services.

Imposing a general obligation to monitor would contradict this framework, as it would render platforms perpetually liable for any illegality, given they would be expected to be always aware of such activities.

This principle has generally been interpreted to mean that intermediary services providers cannot be required to proactively search and filter out illegal content on their platforms.

The question here is: without imposing a general monitoring obligation (GMO), to what extent can an injunction be issued against a platform to prevent illegal activity? Can an obligation be imposed to prevent future infringements? A specific obligation that could be imposed is ensuring that the same seller does not repeatedly sell counterfeit products. This targeted approach aligns with the law's goal of creating a safe and trustworthy online environment, as consumers have the right to a secure platform, and maintaining trust with consumers is crucial.

Can a trademark owner place the responsibility on a platform to protect their trademark themselves?

However, **Article 14(3)** notes that "*This Article shall not affect the possibility for a court or administrative authority, in accordance with Member States' legal systems, of requiring the service provider to terminate or prevent an infringement, nor does it affect the possibility for Member States of establishing procedures governing the removal or disabling of access to information*."

Similarly, under **Article 8** of the DSA, it outlines that no general obligation to monitor the information which providers of intermediary services transmit or store, nor actively to seek facts or circumstances indicating illegal activity shall be imposed on those providers. Therefore, platforms are being held more responsible but nevertheless the court cannot go as

far as to impose a GMO and the principle that no knowledge/awareness of illegal activity means the platform will benefit from immunity from liability stands.

Nevertheless, we consider how under **Article 6(3)** of the DSA, there is slightly more responsibility placed on the online platforms considering that it uses the perspective of the average consumer and argues that if a consumer is led to believe that the information is provided by the platform itself or a recipient acting under its authority, the platform cannot benefit from immunity from liability. This aims to provide checks vis-à-vis the power of online intermediaries, given their significant impact on trade. The law ensures that they are accountable for the information presented and the activities faciltiated on the site.

> *Paragraph 1 shall not apply with respect to the liability under consumer protection law of online platforms that allow consumers to conclude distance contracts with traders, where such an online platform presents the specific item of information or otherwise enables the specific transaction at issue in a way that would lead an average consumer to believe that the information, or the product or service that is the object of the transaction, is provided either by the online platform itself or by a recipient of the service who is acting under its authority or control.*

This is the only difference that exists between it and **Article 14** of the Electronic Commerce Directive.

Looking more closely at the DSA, we take into account the following provisions:

Article 9 speaks about court orders to act against illegal content. This article empowers courts to issue orders requiring platforms to take action against illegal content. It provides a legal framework for ensuring that harmful or unlawful material is promptly addressed, thereby enhancing the safety and legality of online environments. On the receipt of an order to act against illegal content issued by a judicial or administrative authority, an intermediary service provider must inform the issuing authority (or any other authority specified in the order) of '*any effec*t' given to the order without undue delay, specifying if and when effect was given. The authority then informs the Digital Services Coordinator and there is a system where the DSCs around the EU are informed for more harmonisation, as per **Article 9(4)**. In this regard, **Article 9(2)** contains what the order to act against illegal content must contain.

Article 10 discusses court orders to provide information. Therefore, **Article 10** enables courts to issue orders compelling platforms to provide information. This can include data about users or specific content, assisting in the investigation and prosecution of illegal activities. This provision ensures that necessary information can be obtained to uphold the law.

Article 16 deals with notice and action mechansisms where we note that under the ECD**,** implementing notice and action mechanisms was optional for Member States. However, the Digital Services Act (DSA) has standardised this requirement across Europe. This harmonisation ties back to administrative law principles and the concept of due process. By

informing parties and providing reasons for actions taken, the process ensures transparency and accountability. It allows affected parties to challenge decisions, upholding fair procedural standards.

Article 17 concerns the need to issue a statement of reasons, mandating that platforms provide a clear statement of reasons when they take action against content or users. It ensures transparency and allows users to understand the basis for such decisions, thereby enabling them to contest or appeal the actions if they believe them to be unjustified. This is important for the balance of rights and stems from principles of natural justice.

Section 3 DSA provides additional provisions applicable to providers of hosting services, including online platforms, This includes **Article 25** dealing with online interface design and organisation. This mandates that online platforms adhere to specific design and organizational standards for their interfaces. This obligation ensures that platforms are transparent and non-manipulative, enhancing user trust and fairness. While the UCPD and GDPR address many aspects of interface design, the DSA fills in the gaps, providing a comprehensive legal framework. The European Commission's potential guidelines will further assist in the practical application of these rules, particularly in combating dark patterns and ensuring a user-friendly online environment.

The Relationship between the Liability Exemption and EU Consumer Law

While the most relevant case involved an infringement of trademark, the same principles would apply if the underlying law infringed was consumer protection law. The scenarios in which the marketplace can be found liable remain consistent; only the source of the liability changes.

Firstly, it is important to note that neither the ECD nor the DSA stand in the way of the protection of consumers through the EU consumer protection acquis. In fact, **Article 1(3)** of the ECD clarifies the relationship of that Directive with instruments of EU consumer law. This provision states that:

> *This Directive complements Community law applicable to information society services without prejudice to the level of protection for, in particular, public health and consumer interests, as established by Community acts and national legislation implementing them in so far as this does not restrict the freedom to provide information society services.*

Recital 11 further makes clear that the ECD is without prejudice to the level of consumer protection as established by a long list of consumer protection directives.

Similarly, **Article 1(a)(3)(h)** makes it clear that the DSA is without prejudice to the EU consumer protection law acquis. Thus, as is currently the situation under the ECD, the DSA, doesn't preclude consumer law, including the UCPD from extending further protection to consumers. Taking into consideration that the liability exemption for hosting services

remained essentially the same and that the DSA, like the E-commerce Directive, is without prejudice to EU consumer law, it looks like the picture of the liability of online marketplaces under the UCPD as set out in par. III of this article will also be applicable under the DSA.

In relation to the UCPD, we recall that it applies in a B2C context in relation to commercial practices. This means "*any act, omission, course of conduct or representation, commercial communication including advertising and marketing, by a trader, directly connected with the promotion, sale or supply of a product to consumers*", as per **Article 2(d)**. Here, we note that the activities of an online marketplace fall under the definition of a commercial practice. Further, we consider that they also are to be considered within the definition of traders engaging in commercial practices, as per **Article 2(b)**: *any natural or legal person who, in commercial practices covered by this Directive, is acting for purposes relating to his trade, business, craft or profession and anyone acting in the name of or on behalf of a trader*. Thus, they fall within the understanding.

Having determined that online marketplaces typically quali- fy as traders and the offers on their platforms typically qualify as commercial practices, it is now time to turn to the possible grounds for liability under the UCPD.

Liability vis-à-vis Specific Information Duties under Article 7(4) UCPD

The first ground of liability that will be discussed is one that was recently introduced to the UCPD by the Modernisation Directive, and which specifically applies to online market- places. One of the underlying aims of this directive was to bring EU consumer law (including the UCPD) up to date with technological and societal developments, including the shift from offline to online marketing and purchasing in recent years. The Modernisation Directive introduced a specific information duty in the UCPD for online marketplaces in the form of **Article 7(4)(f)** of the UCPD which is one of the articles dealing with misleading omissions. For offers on online marketplaces, the online marketplace will have to indicate whether the seller is a trader or not. The online marketplace can provide this information on the basis of the declaration of that third-party to the online marketplace. Hence, there will not be a duty for the online marketplace to check whether the declaration provided by the third-party is correct.

There can be little doubt that the liability exemption of **Article 14** of the ECD does not preclude liability of online marketplaces on the basis of **Article 7(4)(f) UCPD**. The latter clearly introduces an obligation for the online marketplace itself, rather than holding the online marketplace liable for storage of information provided by the seller on the platform. In addition, even if **Article 14** of the ECD would preclude platform liability in this case, it follows clearly from Article 1(3) of the ECD that it cannot stand in the way of the protection of consumers through EU consumer law. Therefore, the UCPD obliges trader to provide this information and otherwise there will be liability as such will be a misleading omission violating the UCPD, regardless of the ECD.

Liability for other types of 'Own Conduct' under the UCPD

The UCPD Guidance rightly points out that these obligations concern the "own conduct" of the online marketplace rather than illegal information stored at the request of third parties, and that the platforms can therefore not invoke **Article 14** of the ECD against liability. In other words, the online marketplace has an active role, rather than merely being held liable for information stored on its platform by a seller. In addition, even if this argument would not rule out invoking **Article 14** of the ECD, it is again relevant that the ECD does not stand in the way of the protection of consumer interests on the basis of EU consumer law, as per **Article 1(3)**. The same applies to the obligations in relation to the ranking of search results and online reviews, as introduced by the Modernisation Directive.

Other grounds of liability in the UCPD can also be relevant for online marketplaces. Firstly, apart from the specific information duty for online platforms, the Modernisation Directive also introduced other obligations that specifically apply to the online context. For example, the Modernisation Directive established an information duty in relation to the ranking of online search results as per Article 7(4)(a). Therefore, when a trader gives consumers the possibility to search for products offered by different traders or by consumers on the basis of a search query, the trader will have to supply general information on the main parameters determining the ranking of the products as presented to the consumer, as well as the relative importance of those parameters as opposed to others. In other words, the trader will have to inform the consumer how it determines the ranking.

In addition, new measures have been introduced for traders that provide access to consumer reviews of products. This includes a duty to inform the consumer "*whether and how the trader ensures that the published reviews originate from consumers who have actually used or purchased the product*", as per **Article 7(6)**. While these rules do not refer specifically to online marketplaces, they are clearly also written for online marketplaces.

Further, online marketplaces have professional diligence obligations under **Article 5 UCPD** tailored to their specific role elucidated under the UCPD Guidance document of the European Commission. For example, they are required to clearly indicate the identity of the trader offering the product to consumers, as outlined in the UCPD Guidelines, paragraph 4.2.2. Additionally, online marketplaces must structure their websites in a manner that enables third-party traders to present information to platform users in compliance with EU marketing and consumer laws, per the UCPD Guidelines, paragraph 4.2.1.

Liability of Online Marketplaces for Breach of the UCPD Caused by the Seller

Here, we question what if the breach of the UCPD is caused by the seller on the platform, for example because it included false or misleading information in the offer? Here, the legal situation is uncertain, but we can at least try to gain some clarity, depending on the scenario at hand.

We consider three different scenarios:

Scenario 1: If the breach of the UCPD is caused by the seller, but the online marketplace either shares responsibility for the breach or is aware of it but fails to take appropriate action, the marketplace can be held liable for the infringement of the law caused by the seller. In this situation, the online marketplace can essentially be seen as negligent, which makes it feasible to conclude that the online marketplace is acting contrary to professional diligence (**Article 5 UCPD**) or, if co-responsible for misleading the consumer, is liable for conducting a misleading commercial practice (**Article 6 UCPD**). For example: a third-party seller is offering facial masks through an online market- place. It praises the masks for having "the highest level of protection against Covid 19", while the facial masks in reality provide inferior protection compared to most masks on the market. If the online marketplace adds a label stating "Best choice for high protection! It will be co-responsible, and therefore liable under **Article 6 UCPD**.

Scenario 2: When the breach of the UCPD is caused by the seller, and the online marketplace is neither involved in nor aware of the breach, yet the platform plays an *'active role'* as defined by CJEU case law on **Article 14** of the ECD, further analysis is required to determine the extent of this active role. If the platform engages in actions like promoting the seller's offers, rating the seller as a top seller, or sending push emails to advertise the product, they may lose immunity from liability. Therefore, this is determined on a case-by-case basis depending on how active a role the marketplace played. Yet, because of the active role of the online marketplace, it is clear that the liability exemptions in the ECD do not preclude liability of the online marketplace on the basis of the UCPD. Hence, the potential liability of the online marketplace should be determined on the basis of the UCPD itself. Interestingly, one could argue on the basis of the text of the UCPD that an online marketplace that plays an "*active role*" can always be held liable for misleading or aggressive commercial practices on its platform, even though there are also arguments against this.

Scenario 3: If the breach of the UCPD is caused by the seller, and the online marketplace is not involved in or aware of the breach and does not play an 'active role,' it qualifies for immunity from liability. Here, the relationship between the UCPD and the ECD becomes particularly relevant, and it seems likely that the liability exemptions in the ECD (at least indirectly) preclude liability of the online marketplace on the basis of the UCPD. This is also the position taken by the European Commission in the UCPD Guidance. In essence, the European Commission argues that the UCPD should be interpreted in a way that is in line with the regime of liability exemptions of the ECD and the underlying CJEU case law.

Both in scenario 2 and scenario 3, the problem remains that, on the basis of the CJEU case law, the notion of "active role" remains quite unclear. As indicated it is clear from the CJEU case law that the online platform is not exempted from liability if it optimises the presentation of the offers for sale or promotes them, but it is much less clear when this is the case. Clarification of this notion was provided to a degree through Recital 18 of the DSA:

> *The exemptions from liability established in this Regulation should not apply where, instead of confining itself to providing the services neutrally by a merely technical and automatic processing of the information provided by the recipient of the service, the provider of intermediary services plays an active role of such a kind as to give it knowledge of, or control over, that information. Those exemptions should accordingly not be available in respect of liability relating to information provided not by the recipient of the service but by the provider of the intermediary service itself, including where the information has been developed under the editorial responsibility of that provider.*

We also consider how under the DSA, through **Article 6(3)** as noted, we discuss the immunity of hosting liability and its relation with consumer protection law, taken considering the average consumer. It notes that if one has the impression as a consumer that one is dealing with an online marketplace directly, then the online marketplace is not exempt from liability to protect the consumer. This discussion shows that despite the liability ex- emptions in the E-commerce Directive and the draft Digital Services Act, the UCPD provides significant room to hold online marketplaces liable. Both the ECD and the DSA allow for a sectoral approach for consumer law to further address issues in relation to online intermediaries. Hence, despite the fact that the DSA presents a new legal framework for online intermediaries, this framework is by no means the final answer in terms of consumer protection in relation to the sale of products through online marketplaces