Sara Rigazio is a tenure-track researcher in Private Comparative Law at the Department of Political Science and International Relations of the University of Palermo, Italy. She holds a PhD in Private Law and an LL.M. from the University of Minnesota Law School, USA. She has been a visiting fellow at the Norwegian Center for Computer and Law at the University of Oslo and a visiting professor at the Faculté de droit at Lille Catholique University. Her research focuses on vulnerability in the digital environment in relation to new technologies. She has published two books on the empowerment of minors and technology, as well as several articles on privacy, AI, family law, national and international child protection, and legal design.
Contact: sara.rigazio@unipa.it

Soft Power
Revista euro-americana de teoría
e historia de la política y del derecho

Vol. 12(1). Enero-Junio 2025
ISSN (online): 2539/2239 ISSN (print): 2389-8232
https://doi.org/10.14718/SoftPower.2025.12.1.5

IT'S NOT JUST A VIDEO GAME. *FORTNITE* AND THE CASE OF DARK PATTERNS: THE ROLE OF DESIGN STANDARDS IN PROTECTING CHILDREN ONLINE*

Sara Rigazio
Università di Palermo

NO ES SOLO UN VIDEOJUEGO. *FORTNITE* Y EL CASO DE LOS PATRONES OSCUROS: EL PAPEL DE LAS NORMAS DE DISEÑO EN LA PROTECCIÓN DE MENORES EN INTERNET

Abstract
The US Federal Trade Commission (FTC) secured one of the highest agreements in its history against Epic Games Inc., the creator of the popular hit video game *Fortnite*, for violating the Children's Online Privacy Protection Act (COPPA) and the FTC Act. Part

* Reception date: 12th february, 2025; acceptance date: 13th march, 2025. The essay is the result of research carried out within the Dipartimento di Scienze Politiche e delle Relazioni Internazionali, Università di Palermo.

of the complaint regarded deploying "deceptive" design techniques—namely dark patterns—to manipulate users, mostly of them minors. This paper examines the complex topic of dark patterns in relation to children through an analysis of this case and the taxonomy proposed by international institutions. It advances the idea that protecting children in the digital environment can be achieved only through their empowerment, as exemplified by the UK Age-Appropriate Design Code. The article shows that the empowerment of the individual goes hand in hand with the empowerment of the collectivity, calling for a robust response to preserve what dark patterns specifically aim at destroying: the autonomy and identity of the person.

Keywords
dark patterns; Convention on the Rights of the Child (CRC); UK Age-Appropriate Design Code; vulnerability; autonomy.

Resumen
La Comisión Federal de Comercio de los Estados Unidos (FTC) logró uno de los acuerdos más elevados de su historia contra Epic Games Inc., la creadora del popular videojuego *Fortnite*, por violar la Ley de Protección de la Privacidad Infantil en Línea (COPPA) y la Ley de la FTC. Parte de la denuncia se refería al despliegue de técnicas de diseño "engañosas" —en concreto, patrones oscuros— para manipular a los usuarios, en su mayoría menores de edad. Este artículo explora el complejo tema de los patrones oscuros en relación con los niños mediante el análisis de este caso y de la taxonomía propuesta por las instituciones internacionales. También promueve la idea de que la protección de los niños en el entorno digital solo puede lograrse mediante su empoderamiento, como en el caso del Código de Diseño Adecuado a la Edad del Reino Unido. El artículo demuestra que el empoderamiento del individuo va de la mano del empoderamiento de la colectividad, lo que exige una respuesta contundente para preservar lo que los patrones oscuros pretenden destruir específicamente: la autonomía y la identidad de la persona.

Palabras clave
patrones oscuros; Convención sobre los Derechos del Niño (CDN); Código de Diseño Adecuado a la Edad del Reino Unido; vulnerabilidad; autonomía.

Introduction

On December 19, 2022, the US Federal Trade Commission (FTC) obtained from Epic Games Inc., the creator of the popular video game *Fortnite*, a total of $520 million in response to the allegations that the company had violated the Children's Online Privacy Protection Act (COPPA) and the FTC Act.

Regarding the violation of COPPA, the FTC alleges that Epic collected information from players under 13 years old without notifying or obtaining their parents' consent, as required, since *Fortnite* is a child-directed online service.[1] Moreover, the FTC asked Epic to change its default settings concerning voice and text communication for children and teens, since it often resulted in episodes of bullying and harassment of players, exposing them to traumatizing issues and sometimes leading to extreme acts.[2]

Regarding the violation of the FTC Act, in a separate administrative complaint, the FTC alleges that Epic deployed *dark patterns* to manipulate users into making unwanted purchases, specifically allowing children to incur unauthorized charges without parental involvement. In fact, players were often confused by the inconsistent, counterintuitive game settings, which led to unwanted charges when they simply clicked a button.

Dark patterns or deceptive design typically refer to practices that manipulate users into doing something they would not have done without the deceptive design (Leiser, 2023). Despite the term being coined over a decade ago by scholar Harry Brignull (2023), interest in understanding and preventing the use of these practices has only grown in the last few years among academics, regulators, and designers (Gray et al., 2024). Indeed, the term has been codified in several pieces of legislation in Europe and overseas, as well as by international organizations.[3] Therefore, dark patterns are now an emerging concern worldwide. With regard to minors, as the *Fortnite* case shows, concerns rise since the manipulation here exploits individuals who are still at a developmental stage in their personality, character, and

---

[1] See Children's Online Privacy Protection Act at https://www.ftc.gov/legal-library/browse/rules/childrens-online-privacy-protection-rule-coppa. COPPA imposes certain requirements on operators of websites or online services aimed at children under 13 years of age, as well as on operators of other websites or online services that have actual knowledge of collecting personal information online from children under 13 years of age.

[2] According to the FTC's findings, Epic's role in matching children and teens with strangers to play *Fortnite* together harmed children and teens to the point that one of them committed suicide.

[3] The EU does not have a single legislation that regulates dark patterns, but there are multiple regulations that discuss these techniques, and that may be used as a tool to protect consumers. Among these regulations, the most recent is the Digital Services Act (DSA), which entered into force on 16 November 2022 and has been in effect since 17 February 2024. It expressly bans dark patterns in art. Article 25 and Article 31. Among the other EU institutions, the European Data Protection Board (EDPB) issued guidelines in March 2022 on deceptive design, which were adopted on 14 February 2023. Also overseas, the US FTC stepped in and, following a 2021 public workshop, published a staff report in 2022. Finally, the Organization for Economic Co-operation and Development (OECD) also intervened in October 2022.

emotions, with the consequence of increasing their vulnerability (Hartzgov, 2018, p. 131; Malgieri & Niklas, 2020).

The response of institutions, on a global scale, has been primarily realized through enforcement actions related to privacy violations and, in the case of children, through consumer protection law, mainly to defend their parents' economic interests.

This article argues that the specific topic of dark patterns in services (likely to be) accessed by minors, as well as the more general matter of the protection of children in the digital environment, should be addressed primarily from the children's rights perspective. It suggests that the response should be robust in its design (Hartzgov, 2018, p. 183) and that the legal parameters to consider are principally found in the Convention on the Rights of the Child (CRC). These arguments are advanced using *Fortnite* as a case study and the standards set out in the 2020 UK Age-Appropriate Design Code. The core idea proposed here is that there can be no real protection on the Internet without the real promotion of users' rights (and duties), and this can only be achieved by empowering individuals in the first place. At the same time, I argue that the involvement of all actors in the digital environment is equally necessary to empower the collectivity. Protecting children's rights on the Internet is consistent with this argument.

The article is organized as follows: the first part briefly presents the FTC decision on *Fortnite* and introduces the topic of dark patterns. The second part addresses the main issues arising in relation to children's rights and analyzes the solution proposed in the UK.

The *Fortnite* case

Fortnite is a highly popular video game among kids, produced by Epic Games Inc., a US-based corporation headquartered in Maryland. *Fortnite* itself is free to download and play; however, Epic charges users for certain in-game items, such as costumes and utilities. The problems began when, in most cases, Epic deployed a series of "design tricks"—as defined by the FTC—known as dark patterns to charge customers for these items without first obtaining their consent. Moreover, after the charge was processed, Epic denied users access to the prepaid content when they disputed the unauthorized charges with their credit card providers. Additionally, after the first purchase, Epic recorded consumers' payment information and used it for future charges, including those made by children. It is worth noting that many customers were unaware that their card had been saved by Epic.

As previously mentioned, part of the FTC's investigation focused on the modalities through which Epic charged its customers, i.e., *the dark patterns*. As a matter of fact, unintentional purchases were the result of a precise policy of design systematically

tailored for this purpose (Bösch et al., 2016). It is therefore important to understand how this works in *Fortnite* since it represents a clear example of how dark patterns operate in general (Consumer Protection Cooperation Network, 2022).

The game's start screen is designed so that the start button is clearly highlighted in yellow, with the word "free" immediately above it. Only when the user continues by scrolling down the page will they read, in small print, a range of information, such as the game's age rating and the option to make purchases. Furthermore, once started, the game allows users to "embellish" the appearance of characters using a series of tools (outfits, dance moves, and other in-game content) that can be obtained by simply clicking a button, without any authorization or consent being requested. As a consequence, the cost is immediately charged to the payment method entered during registration, which is saved by default (FTC, 2022, pp. 3, 6).

In addition, the same arrangement of the control buttons on the game console turns out to be reversed in one of *Fortnite's* competitions in comparison to the usual disposal, so that the player thinks to click on the button corresponding to "more information," but instead clicks on the "purchase" button. Among the consumers involved, as said, the majority were minors. Parents downloaded the game for their kids to play, and once done, children could do everything they wanted, including purchasing any items at any price, with a single click, without parents being notified.

Parents began to complain, as reported in the FTC report (FTC, p. 20), and Epic's employees raised concerns about the default method for saving credit card information.

Nevertheless, despite receiving numerous complaints (according to the FTC report, more than one million), Epic had not changed any procedures except in the last period, and likewise, after learning that it was under investigation by the FTC. Moreover, Epic made the situation worse by deliberately obscuring the "cancel and refund" buttons after receiving complaints, rendering the procedure practically impossible. After the investigations, the FTC decided that these deceptive techniques were to be considered under "unfair or deceptive acts or practices in or affecting commerce," as provided by Section 5 of the FTC Act, USC § 45(a). Therefore, the Commission secured the agreements with Epic.

The "Essence" of Dark Patterns

The topic of dark patterns has, in the last few years, inspired a new focus on addressing online information asymmetry (Competition Market Authority [CMA], 2022). Moreover, this topic has become widespread in the scholarly discourse and the public policy debate. Regulators and institutions, at the national and international levels, therefore, embraced the complex task of addressing and outlining it through the definition of a

taxonomy. The difficulty lies in the fact that, as many scholars have pointed out, these patterns range from nudge techniques to coercive ones (Leiser & Santos, 2023; Luguri & Strahilevitz, 2021).

Consequently, I will present key definitions from various international institutions and organizations to highlight their common features.

The European context proves to be a rich ambit in this topic. According to the European Data Protection Board's (EDPB) guidelines issued in 2022, dark patterns are "interfaces and user experiences implemented on social media platforms that lead users into making unintended, unwilling and potentially harmful decisions in regard to their personal data with the aim of influencing users' behaviors" (EDPB, 2022). In addition, the EDPB also identifies six categories of dark patterns: 1) overloading, 2) skipping, 3) stirring, 4) obstructing, 5) fickle, and 6) left in the dark. The legal basis recalled by the EDPB is to be found in the GDPR, specifically in Articles 5, 4, and 7 regarding consent, as well as in Article 12 regarding transparency. Article 25 then plays a critical role in privacy by design and by default. In this regard, the guidelines also underline specific elements to be considered in relation to this provision when dealing with dark patterns, which are: autonomy, interaction, expectation, consumer choice, power balance, no deception, and truthful.

The Digital Services Act (DSA), whose rules have fully applied since February 2024, specifically prohibits deceptive or nudging techniques and gives the Commission the power to adopt delegated acts to define additional techniques that could be included in the notion of dark patterns. The decisive criterion here is that the user's freedom of choice is distorted or impaired (see Article 25(1) of the DSA).

While the Digital Markets Act (DMA) does not explicitly mention dark patterns, it imposes obligations on gatekeepers that can also be referred to as dark patterns. Indeed, it stipulates that online interfaces should not be designed in a manipulative manner to impair users' ability to freely consent to the service (European Union, 2022, Article 37).

Also, the Unfair Commercial Practices Directive (UCPD) is relevant since it prohibits unfair commercial practices affecting consumers' economic interests before, during, and after the conclusion of a contract. In December 2021, the European Commission published guidance on the UCPD that confirms that the directive covers dark patterns and dedicates a section (4.2.7) to explain how these provisions can be applied to consumers.

The AI Act (as in the final draft approved on December 8, 2023) addresses dark patterns in Article 5, stating that "subliminal techniques beyond a person's consciousness or purposefully manipulative or deceptive techniques, with the objective to or the effect of materially distorting a person's or a group of persons' behaviour […]" are prohibited. The

provision also emphasizes the connection to vulnerabilities that may be exploited and expressly refers to factors such as age, disability, or specific economic or social conditions. Finally, regarding the target audience of children, it is worth noting that on June 14, 2022, the EDPB and the Consumer Protection Cooperation (CPC), together with several national data protection authorities, issued the Joint Principles for Fair Advertising to Children. This is a list of five key principles for advertising directed at children, including, among others, the prohibition on designing interfaces that prompt kids to purchase in-game content (such as in *Fortnite*).

More generally, it can be said that the EU is taking, and has already taken, several steps forward in regulating dark patterns, with a clear, far-reaching perspective, given the multiple legislative frameworks involved.

Other relevant initiatives include the report prepared in 2022 by the US FTC, entitled "Bringing dark patterns to light," where the federal agency, through a public workshop, investigated the phenomenon of manipulative techniques and showed many examples of dark patterns operating on the Internet, in a similar way to the EPDB classification. The report dedicated a specific section to children regarding the "Design Elements that Lead to Unauthorized Charges" (Federal Trade Commission, 2022, p. 10), citing examples of in-app charges from Google,[4] Amazon,[5] and Apple.[6]

In 2022, the Organisation for Economic Co-operation and Development (OECD) also published a paper, *Dark commercial patterns*, where it proposed a working definition and identified possible policies and enforcement responses to mitigate dark commercial patterns (OECD, 2022, p. 2). The OECD's definition indeed highlights the subversion or impairment of the consumer's autonomy, leading to detriment in various ways.[7] In accordance with this thrust, it also identifies another important element in the taxonomy of dark patterns: namely, the vulnerability referred to minors, declined, however, taking into account not only inherent factors (the age, for example) but also situational (the socioeconomic conditions, the level of education) (Mendola & Pera, 2021). In this way, the paper's findings reveal that minors from lower socio-economic strata played apps with more manipulative designs (OECD, 2022, p. 55).

---

[4] *In the Matter of Google Inc*., Docket No. C-4499.

[5] *FTC v. Amazon.com Inc*., Case No. 2:14-cv-01038 (W.D. Wash.).

[6] *In the Matter of Apple Inc.,* Docket No. C-4444.

[7] According to the OECD (2022), the working definition of dark pattern is: "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 many instances" (p. 5).

Although the taxonomies identified and briefly reported naturally display some differences between them, it is nevertheless possible to trace a common and uniform line and, above all, an element that I consider essential to the specific topic here being addressed. At the same time, this element may well relate to the relationship with the digital dimension more generally.

The element I am referring to is the effect that dark patterns have on the user's identity, specifically the complete *depersonalization* (European Commission: Directorate-General for Justice and Consumers, 2022). As the studies and reports noted above have shown, these manipulative techniques induce the subject to take actions and make decisions that the user would otherwise never have taken (Gunawan et al., 2021). Moreover, dark patterns increase vulnerability in its twofold dimensions: the inherent, which relies on the intrinsic characteristics of the human nature, connected to corporeality and dependent on others affective and social natures, and the situational, which depends on economic or environmental circumstances within which individuals or social groups live in, including oppression, domination, and injustice (Gray et al., 2018; Mackenzie et al., 2014, p. 29). In the words of Stefano Rodotà (2012), "physical integrity is respected, but the integrity of the person, and with them his or her autonomy, are diminished"[8] (p. 315).

In this respect, it is necessary to examine the children's dimension, focusing on the rights of minors from a child-centered perspective and on children's empowerment. This can be possible through the legal instruments provided for in the CRC.

The "Revolutionary" Idea of the Minor in the CRC

The CRC was approved by the United Nations General Assembly on 20 November 1989 and entered into force on 2 September 1990. Currently, it is the most widely recognized and ratified international document, with the sole exception of the United States of America. The principle that drives the Convention is that the child is no longer an object of others' decisions (mainly the parents), according to a patriarchal idea of family, but must be considered an individual fully entitled to a series of rights (as well as duties) that contribute to the ever-evolving formation of their identity.

This implies that all choices affecting the child, as covered by Article 3 of the CRC, must be made in accordance with the best interests, which constitute the only driving principle of every action concerning children. Moreover, it is worth noting that this provision, as well as the entire Convention, is directed at both public actors, such as states, and private actors, including business operators and other organizations.

---

[8] *"L'integrità fisica è rispettata, ma l'integrità della persona, e con essa la sua autonomia, sono continuamente ridotte".*

The revolutionary impact of the Convention is embodied in the concept of protection. This term takes on an entirely different meaning than before: it is not identified in mere interdictions, in prohibitions anymore, but instead, on the basis of the new conception of the child embedded in the CRC, it implies a new interaction between the child and the context in which life and daily activities take place. In this respect, the Convention is based on the fundamental principle that the child's *evolving capacities* should be recognized in accordance with the level of maturity demonstrated (Lansdown, 2005). These capacities increase progressively toward autonomy, not only with age alone, but also with the child's awareness of the consequences of their actions and the risks involved. In fact, evolving capacities are not dependent solely on age (CRC, 2023). And this is where the real revolutionary profile lies: autonomy means being aware and assuming responsibilities—individually and collectively—and, therefore, implies duties; it is certainly not a matter of accommodating mere whims.

This process is made possible only if the child is provided with all the necessary instruments to fully exercise their rights under the CRC. This means, therefore, that first the family and then the institutions, together with all the actors involved, share a concrete and collective responsibility in this process. For example, it means creating the right circumstances in which the child can "prove" their autonomy without incurring risks inappropriate to their level of maturity.

From this perspective, then, the actions that, in the specific case of *Fortnite* and, more generally, the platforms, put in place through dark patterns are even more illegitimate. It is evident that deceptive and manipulative acts, such as the ones described in *Fortnite*, aim at diminishing the autonomy, but these acts take advantage not only just of the vulnerable condition of *any* user (and even in this case, they are to condemn)—but of users that are still discovering, maturing, getting to know and choosing their own personality. In so doing, often in an underhanded way, dark patterns violate this peculiar process in the child's development, since they affect their evolving capacities and, therefore, the construction of their autonomy, inducing the minor to make decisions that are not the result of free considerations but, rather, of real coercion.

In this respect, I think the response, as mentioned above, should be implemented at two levels. Individually, through an action of empowerment of the child, and collectively, through an action of awareness and empowerment among the collectivity of "education"—about the necessity of assuming a child's rights perspective when we talk about topics that concern children.

The commitment necessary for this response has recently increased thanks to the strong dedication shown in particular by some children's organizations, such as the En-

glish 5RightsFoundation, which leads to a bigger worldwide movement in support of the protection and promotion of children's rights in the digital environment, and literally pushes for a real and concrete change in this ambit. Indeed, at a general level, it is worth noting General Comment No. 25 by the Committee on the Rights of the Child, which underscores the international community's commitment to recognizing the same rights embedded in the CRC in the digital environment.[9] At the same time, the EU has initiated a series of measures to approve a European Children's Code, modeled after the English one.[10] As a matter of fact, on a specific level, the UK Age-Appropriate Design Code (or Children's Code), with its standard specifically aimed at dark patterns, is exactly the proof of this commitment.

The UK Age-Appropriate Design Code and the Standard on Dark Patterns

The UK Age-Appropriate Design Code entered into force in September 2020. It has been the first regulatory text on children's protection in the digital environment to establish a set of design standards aimed principally at digital platforms offering services *likely* to be accessed by children. These standards provide built-in protections that allow children to learn, play, and explore on the web, ensuring that their best interests are always the primary consideration in the design and development of online services. Indeed, these standards explicitly recall the core principles of the UN Convention, providing further confirmation that the Code is deeply rooted in the CRC.

Practically, this means, *inter alia*, strong privacy by default, geolocation services switched off by default, and a minimum amount of information about children collected and retained by the platforms.[11]

Regarding dark patterns, the Code allocates a specific standard to this topic. Standard 13 is entitled "Nudge techniques" and is defined as: "design features which lead or encourage users to follow the designer's preferred paths in the user's decision making." Moreover, the Code expressly mentions techniques to encourage children to provide or share unnecessary

---

[9] See CRC/C/GC/25 (https://www.ohchr.org/en/documents/general-comments-and-recommendations/general-comment-no-25-2021-childrens-rights-relation).

[10] As early as 2012 the Commission launched the "Better Internet for kids – BIK+" initiative, which consisted of a real strategy of action on four main guidelines, concerning the quality of online content aimed at minors, the awareness and subsequent empowerment of minors themselves, the creation of a safe digital environment and, finally, the fight against sexual abuse and the dissemination of child pornography online. The 2012 BIK+ strategy was updated in 2022 in light of the imminent passage of the Digital Services Act and the commitment made in the proposed regulation on the European Digital Identity (EDi). In December 2022, in fact, a call was launched to identify the members of the group that will draft the EU Age-Appropriate Design Code by early 2024.

[11] The standards of the Code are: *best interest of the child; data protection impact assessments; age-appropriate application; transparency; detrimental use of data; policies and community standards; default settings; data minimization; data sharing; geolocation; parental controls; profiling; nudge techniques; connected toys and devices; online tools.*

personal data or turn off the default privacy protections. It is evident that the Code refers to deceptive or manipulative techniques, and therefore, to dark patterns.

In addition, the Code provides some practical examples to show how these techniques could work and appear: for example, how the screen and the choice of colors could indeed encourage or induce the child to make decisions that are detrimental to the privacy settings (as recalled in *Fortnite*), lowering their default higher protections or, simply by clicking, purchasing extra items unnecessary to the service requested.

The profile I would like to underline is that, at the same time, next to banning the use of dark patterns, the Code endorses a pro-active approach: for example, it invites providers to use pro-privacy nudges (or, patterns) according to the age and maturity of the child, starting from nudges towards high privacy options when there is a limited level of understanding, getting to more neutral interventions that require minors to think things through. The proactive side of this standard is further promoted by suggesting that nudges could support children's health and well-being or invite them to use tools or resources, such as pause and save buttons. All these recommendations are based on the premise that providers should act solely in children's best interests and take into account users' levels of maturity, providing different options accordingly.

Therefore, the UK Children's Code provides practical, concrete guidance to providers on dark patterns. Despite providing a broader definition of these techniques than those in EU legislation and the US FTC, the UK's approach appears more effective in this respect.

Indeed, it is completely in line with the rationale of the CRC and the principle of evolving capacities, and at the same time, calls for the robust response I mentioned above by the institutions, service providers, and the family. From this perspective, indeed, the Code regulates a severe system of enforcement and sanctions, in line with what Woodrow Hartzog (2018) defines as a robust decision by lawmakers and regulators: "one that directly and significantly punishes bad design or dictates design specifics" (p. 184). Moreover, the "powerful incentives" recalled by Hartzog are present in the case of the Code, suggesting that *clear patterns*, rather than dark ones, create a virtuous circuit that could, potentially, become an example and a best practice. On the other hand, the family's involvement through parental control confirms the Code's commitment to the CRC and its aim of protecting the child and promoting their rights. The Code is a clear example of how the CRC principles have been completely embedded, taking into consideration the characteristics of the digital environment. As a matter of fact, the aim of the Code is not "to protect children from the digital world, but […] protecting them within it."

Ways Forward and Conclusions

In the previous pages, I tried to explore how dark patterns represent a real and concrete harm to children's rights. The example set in the *Fortnite* case study demonstrated how easily manipulative techniques can be deployed and, therefore, how critical it is to identify and ban them from the digital domain.

Dark patterns, deceptive design, or nudge techniques are dangerous, and this is a fact. But the element that I tried to highlight in this paper is that the manipulative effect is deep and even brutal on the user since it hits the very essence of the human being: the identity and, consequently, the autonomy of the person, which is inseparable from the dignity of the person (Rodotà, 2012, p. 315). In this way, the machine, the digital instrument, is no longer a tool because it prevails over the person, *depersonalizing* the human being and eliminating autonomy of choice. Instead, in front of a screen, the user must be free to choose, change their mind, and be well-informed, with all possibilities clear and explained. Otherwise, the person is completely "absorbed by the machine, with a radical change of his prerogatives," as Rodotà (2012, p. 315) clearly points out.

In the case of the minors, the deceptive effect is amplified and more subtle. The *Fortnite* case has shown how even the choice of colors or the position of a button can create a sense of complete dependency and loss in young players.

Dark patterns exploit a user's peculiar condition, which we often refer to as vulnerability. As we all are, minors are inherently and situationally vulnerable as well. Therefore, we have to look at the response we want to give: in the case of dark patterns deployed to children, the instruments are primarily to be found in the CRC. In this way, the law re-establishes the priority of the human side (Rodotà, 2012, p. 317), the autonomy of choice that, for children, is realized through the pursuit of their best interest and the principle of the evolving capacities.

The response must be robust as well: there can be no compromises with the platforms, nor with the rest of the actors involved. There is, indeed, I believe, a collective responsibility in protecting children's rights in the digital environment that go through several and diverse actions: a general awareness about the CRC's rights through a process of "digital education"; the commitment by the institutions in assuming a child's rights perspective and, of course, a series of duties and responsibilities by the minors themselves who, according to their maturity, learn to "move" within the digital environment to take advantage of it for their best interest.

This is how the empowerment of children in the digital environment can be realized: the UK Children's Code shows that this is not only possible but practically achievable. The

robust response is paired with a counterproposal: proactive patterns and clear, "good" techniques to encourage children to fully exercise their rights, thereby making them *citizens* rather than just a source for data mining (Rodotà, 2012, p. 197).

After all, as it has been noticed, the digital environment is the product of humans, and the quality of the digital product does not depend "on some casual and unpredictable event […] but on the quality of the data that is fed into it at the beginning and is continuously collected" (Zeno-Zencovich, 2024, p. 3).

References

Brignull, H. (2023). *Deceptive Patterns: Exposing the Tricks Tech Companies Use to Control You*.

Bösch, C., Erb, B., Kargl, F., Kopp, H., & Pfattheicher, S. (2016). Tales from the Dark Side: Privacy Dark Strategies and Privacy Dark Patterns. *Proceedings on Privacy Enhancing Technologies*, (4), 237–254. https://doi.org/10.1515/popets-2016-0038

Committee on the Rights of the Child. (2023). *Statement of the Committee on the Rights of the Child on Article 5 of the Convention on the Rights of the Child*. https://www.ohchr.org/sites/default/files/documents/hrbodies/crc/statements/CRC-Article-5-statement.pdf

Competition Market Authority (CMA). (2022). *Online Choice Architecture: How digital design can harm competition and consumers*. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1066524/Online_choice_architecture_discussion_paper.pdf

Consumer Protection Cooperation Network. (2022). Cooperation between consumer and data protection authorities. *European Commission*. https://commission.europa.eu/live-work-travel-eu/consumer-rights-and-complaints/enforcement-consumer-protection/cooperation-between-consumer-and-data-protection-authorities_en

European Commission: Directorate-General for Justice and Consumers. (2022). *Behavioural study on unfair commercial practices in the digital environment: dark patterns and manipulative personalisation: final report*. Publications Office of the European Union. https://data.europa.eu/doi/10.2838/859030

European Data Protection Board. (2022). *Guidelines 3/2022 on Dark patterns in social media platform interfaces: How to recognise and avoid them*. https://edpb.europa.

eu/our-work-tools/documents/public-consultations/2022/guidelines-32022-dark-patterns-social-media_en

European Union. (2022). Digital Markets Act. *Official Journal of the European Union*. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022R1925

Federal Trade Commission (FTC). (2022). *Bringing Dark Patterns to Light* [Staff Report]. https://www.ftc.gov/system/files/ftc_gov/pdf/P214800%20Dark%20Patterns%20Report%209.14.2022%20-%20FINAL.pdf

Gray, C. M., Bielova, N., Santos, C., & Mildner, T. (2024). An Ontology of Dark Patterns: Foundations, Definitions, and a Structure for Transdisciplinary Action. *CHI '24: Proceedings of the 2024 CHI Conference on Human Factors in Computing Systems*, 1–22. https://doi.org/10.1145/3613904.3642436

Gray, C. M., Kou, Y., Battles, B., Hoggatt, J., & Toombs, A. L. (2018). The Dark (Patterns) Side of UX Design. *CHI '18: Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*, 1–14. https://doi.org/10.1145/3173574.3174108

Gunawan, J., Choffnes, D., Hartzog, W., & Wilson, C. (2021, May 8–13). *Towards an Understanding of Dark Pattern Privacy Harms*. CHI'21 [Online Virtual Conference]. https://darkpatterns.ccs.neu.edu/pdf/gunawan-2021-chiworkshop.pdf

Hartzgov, W. (2018). *Privacy's blueprint. The Battle to control the design of new technologies*. Harvard University Press.

Lansdown, G. (2005). *The evolving capacities of the child*. Innocenti UNICEF.

Leiser, M., & Santos, C. (2023). Dark Patterns, Enforcement, and the emerging Digital Design Acquis: Manipulation beneath the Interface. *OSF*. https://doi.org/10.31235/osf.io/rf3ja

Luguri, J., & Strahilevitz, L. J. (2021). Shining a Light on Dark Patterns. *Journal of Legal Analysis, 13*(1), 43–109. https://doi.org/10.1093/jla/laaa006

Malgieri, G., & Niklas, J. (2020). Vulnerable data subjects. *Computer Law & Security Review*, *37*, 105–415. https://doi.org/10.1016/j.clsr.2020.105415

Mackenzie, C., Rogers, W., & Dodds, S. (2014). Introduction: What Is Vulnerability and Why Does It Matter for Moral Theory? In W. Rogers, C. Mackenzie, & S. Dodds (Eds), *Vulnerability. New Essays in Ethics and Feminist Philosophy* (pp. 1–29). Oxford University Press. https://doi.org/10.1093/acprof:oso/9780199316649.003.0001

Mendola, D., & Pera, A. (2021). Vulnerability of refugees: Some reflections on definitions and measurement practices. *International Migration*, *60*(5), 108–121. https://doi.org/10.1111/imig.12942

Organisation for Economic Co-operation and Development (OECD). (2022). *Dark Commercial Patterns. OECD Digital Economy Papers.* https://www.oecd.org/con-

tent/dam/oecd/en/publications/reports/2022/10/dark-commercial-patterns_9f-6169cd/44f5e846-en.pdf

Rodotà, S. (2012). *Il diritto di avere diritti*. Laterza Editori.

Zeno- Zencovich V., (2024). Artificial intelligence, natural stupidity and other legal idiocies. *MediaLaws*, 1.