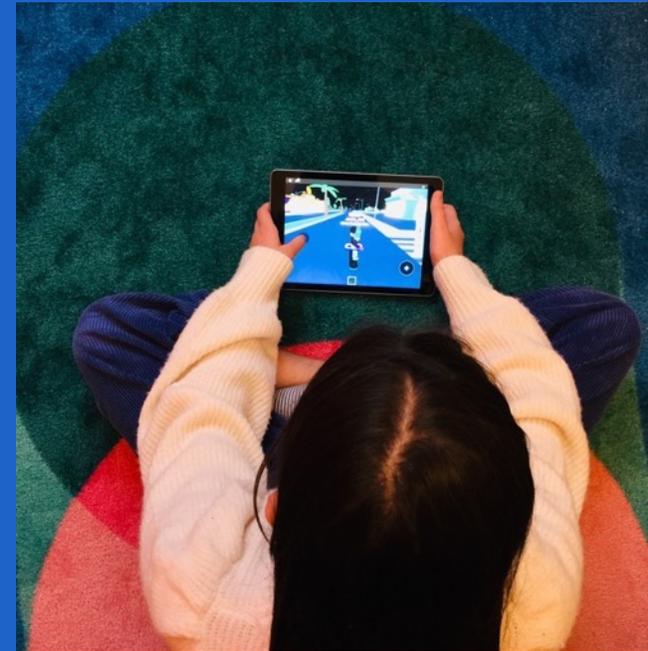


Setting the scene: Consumer risks for children and young people in the digital environment and the regulatory framework

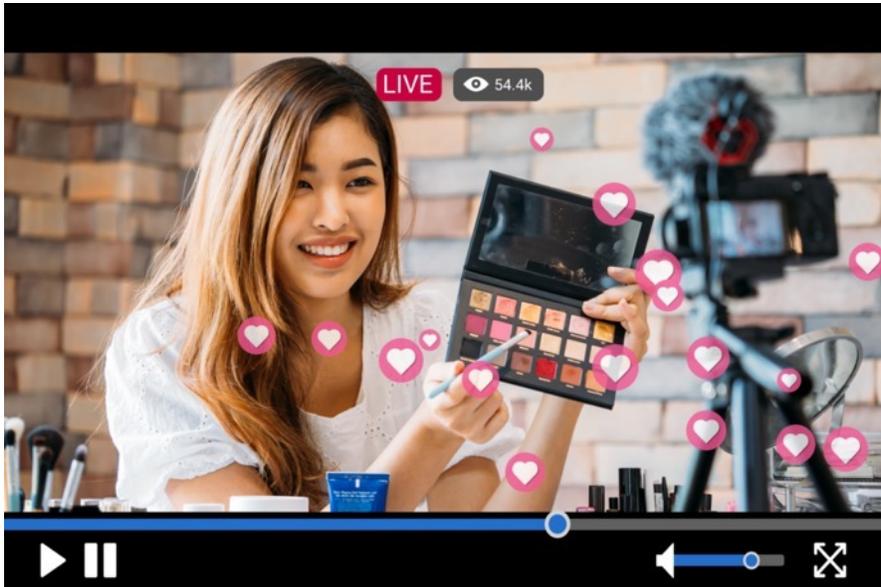
Roundtable on child and youth consumer protection in digital markets (22 September 2022)

Prof. dr. Eva Lievens (Law & Technology)





Picture: iStock



Picture: iStock



	Kids	Youth
	KINDEREN	JONGEREN
YouTube	86%	96%
Netflix	68%	74%
TikTok	56%	86%
Spotify	52%*	75%
WhatsApp	45%	91%
Ketnet	41%	8%
Snapchat	40%	91%
Disney+	38%	23%
Pinterest	37%*	57%
Instagram	28%	83%
Twitch	27%*	25%
YouTube Kids	22%	1%
Facebook	15%	41%
Twitter	15%*	22%
Discord	15%	29%
FB Messenger	10%	49%
Radio websites en radio apps	8%*	6%
Streamz	7%*	11%
iTunes	7%*	4%
Reddit	6%*	11%
Andere	45%	34%

*Niet bevraagd bij kinderen eerste graad lager
 Tabel 8: Gebruik apps of websites door kinderen en jongeren

Source: Apestaartjaren, Research report 2022, <https://www.apestaartiaren.be/>



Picture: iStock



Minecraft

Fortnite

FIFA

Pictures: Unsplash



Source:
https://www.gameable.info/_files/ugd/7f91ff_c197ace0298e44ff8dca0fb124e36b78.pdf

		Games Kids	Games Youth	Social Media Kids	Social Media Youth
		GAMES KINDEREN	GAMES JONGEREN	SOCIALE MEDIA KINDEREN	SOCIALE MEDIA JONGEREN
Mostly not	Meestal NIET	21%	19%	10%	2%
Not every day	Niet elke dag	19%	20%	17%	3%
Less than 1h/day	Minder dan 1u per dag	16%	13%	18%	13%
1-2 h/day	1-2 uren per dag	21%	28%	22%	29%
2-3 h/day	2-3 uren per dag	12%	12%	14%	24%
3-4 h/day	3-4 uren per dag	4%	4%	8%	14%
	Meer dan 4u per dag	7%	4%	11%	15%

Tabel 9: Frequentie gebruik van games en sociale media kinderen en jongeren op een schooldag
 Frequency of use of games and social media kids and youth on a school day

Source: Apestaartjaren, Research report 2022, <https://www.apestaartjaren.be/>



children love social media, video-based platforms and gaming



enormous opportunities for play, leisure, entertainment & creativity



commercial stakes are high



commercial strategies might be difficult to detect



blurring lines between watching, gaming and gambling; and between persuasion and manipulation



children are concerned



concerns about financial risks in online games

paid upgrades during gameplay = very enticing for children

spending large amounts of money without their parents' knowledge

feeling harassed by advertisements in games that promote the installation of gambling apps or contain false notifications of wins

lack of control of advertising in online games

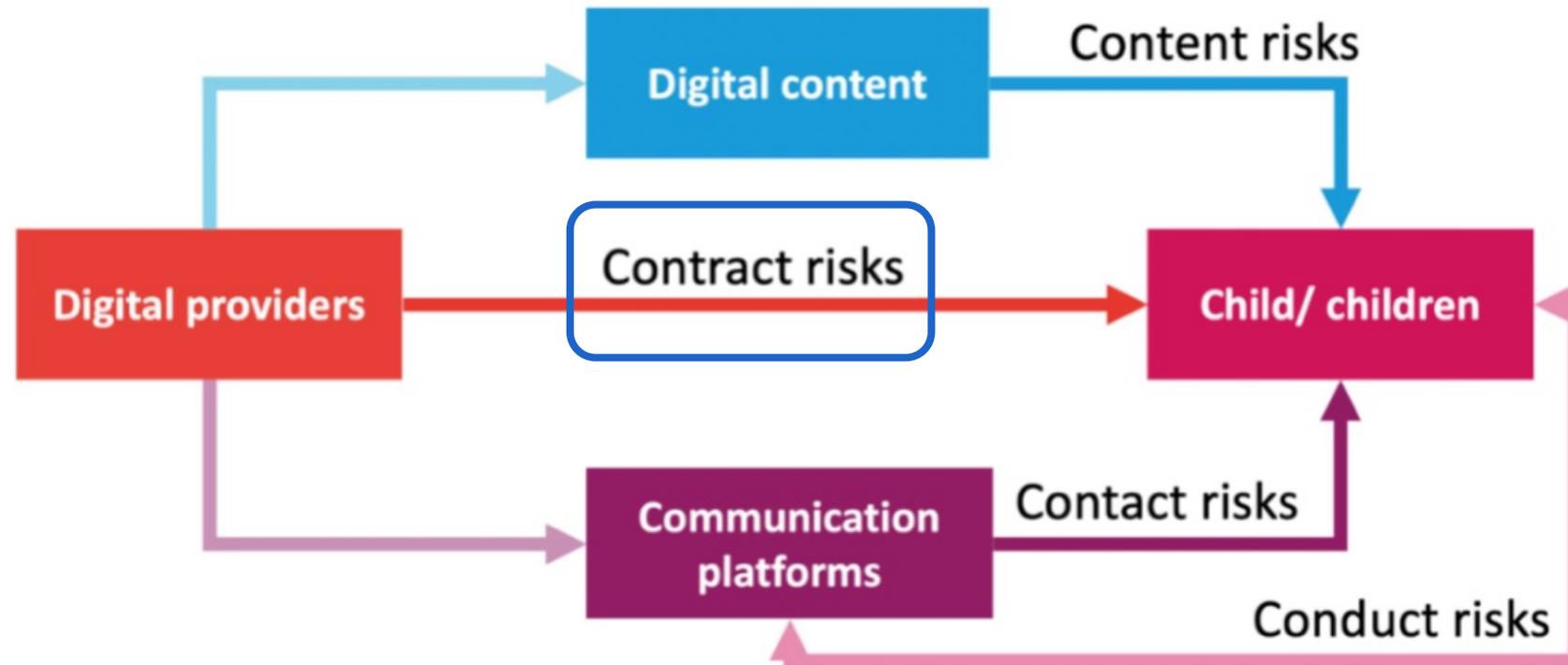
fraud in games

Figure 1: The EU Kids Online original 3Cs classification of online risks (Livingstone et al., 2011)

	Content Receiving mass-produced content	Contact Participating in (adult-initiated) online activity	Conduct Perpetrator or victim in peer-to-peer exchange
Aggressive	Violent/gory content	Harassment, stalking	Bullying, hostile peer activity
Sexual	Pornographic content	'Grooming', sexual abuse or exploitation	Sexual harassment, 'sexting'
Values	Racist/hateful content	Ideological persuasion	Potentially harmful user-generated content
Commercial	Embedded marketing	Personal data misuse	Gambling, copyright infringement

Source: Livingstone, S., & Stoilova, M. (2021). The 4Cs: Classifying Online Risk to Children. (CO:RE Short Report Series on Key Topics). Hamburg: Leibniz-Institut für Medienforschung | Hans-Bredow-Institut (HBI); CO:RE - Children Online: Research and Evidence. <https://doi.org/10.21241/ssoar.71817>

Figure 3: The EU Kids Online 4Cs model of online risks (Livingstone et al., 2020, p. 57, adapted from Hasebrink et al., 2018)



Source: Livingstone, S., & Stoilova, M. (2021). The 4Cs: Classifying Online Risk to Children. (CO:RE Short Report Series on Key Topics). Hamburg: Leibniz-Institut für Medienforschung | Hans-Bredow-Institut (HBI); CO:RE - Children Online: Research and Evidence. <https://doi.org/10.21241/ssoar.71817>



Risks for Children in the Digital Environment				
Risk Categories	Content Risks	Conduct Risks	Contact Risks	Consumer Risks
Cross-cutting Risks	Privacy Risks (Interpersonal, Institutional & Commercial)			
	Advanced Technology Risks (e.g. AI, IoT, Predictive Analytics, Biometrics)			
	Risks on Health & Wellbeing			
Risk Manifestations	Hateful Content	Hateful Behaviour	Hateful Encounters	Marketing Risks
	Harmful Content	Harmful Behaviour	Harmful Encounters	Commercial Risks Profiling
	Illegal Content	Illegal Behaviour	Illegal Encounters	Financial Risks
	Disinformation	User-generated Problematic Behaviour	Other Problematic Encounters	Security Risks

Source: OECD (2021), "Children in the digital environment: Revised typology of risks", OECD Digital Economy Papers, No. 302, OECD Publishing, Paris, <https://doi.org/10.1787/9b8f222e-en>





Guidelines to respect, protect and fulfil the rights of the child in the digital environment

www.coe.int/t/children Building a Europe for and with children

CONSEIL DE L'EUROPE



Brussels, 24.3.2021
COM(2021) 142 final

COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS

EU strategy on the rights of the child



Brussels, 11.5.2022
COM(2022) 212 final

COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS

A Digital Decade for children and youth:
the new European strategy for a better internet for kids (BIK+)

Digital and information society: An EU where children can safely navigate the digital environment, and harness its opportunities



KNOW YOUR RIGHTS IN THE DIGITAL ENVIRONMENT

The UN Committee on the Rights of the Child has just said...

YOUR RIGHTS APPLY IN THE DIGITAL WORLD

YOU HAVE THE RIGHT TO PRIVACY
Digital technologies can help give access to information, but they can also be used to monitor and track you. You have the right to control how your personal information is collected, used and shared.

YOU HAVE A RIGHT TO HEALTH, EDUCATION AND SERVICES
Digital technologies can help give access to information, but they can also be used to monitor and track you. You have the right to control how your personal information is collected, used and shared.

YOU HAVE THE RIGHT TO PARTICIPATE
Digital technologies should not be used to stop you from taking part in decisions that affect your life. You have the right to be heard and to be taken into account.

Information online should be true, clear and understandable to you - in a language you speak

YOU HAVE THE RIGHT TO INFORMATION
You have the right to know what is going on around you. You have the right to be told the truth.

YOU HAVE A RIGHT TO PLAY AND REST
Playing online should not stop you from playing offline. You have the right to rest and to have fun.

YOU HAVE THE RIGHT TO BE SAFE
You should not be harassed, bullied or abused online. You have the right to be safe.

YOU HAVE THE RIGHT NOT TO BE EXPLOITED
Digital technologies should not be used to exploit you. You have the right to be protected from exploitation.

YOU HAVE THE RIGHT TO BE HEARD
You should be listened to and your views should be taken into account. You have the right to be heard.

MOST OF ALL, YOU HAVE THE RIGHT TO BE YOU
You should be able to be yourself online. You have the right to be you.

And your rights apply whenever you are, wherever you live, whatever your shape, age, gender, religion, race or beliefs.

BRIGHTS FOUNDATION
BrightsFoundation.com



Children today spend an increasing part of their lives online: since 2011, the number of 12- to 15-year-olds who own smartphones has increased by more than 50%. The digital environment offers tremendous benefits to children, opening new channels for education, creativity and social interaction. But it also presents serious risks, including cyberbullying, sextortion and risks to privacy. These risks have become particularly acute amid the COVID-19 crisis and the surge in screen time it has precipitated.

The **OECD Recommendation on Children in the Digital Environment**, adopted in May 2021, aims to help countries to find a balance between protecting children from online risks, and promoting the opportunities and benefits that the digital world provides. The Recommendation sets out principles for promoting a safe and beneficial digital environment for children, recommendations on overarching policy frameworks, and highlights the importance of international co-operation.



> [Read the Recommendation in English](#)

> [Lire la Recommandation en français](#)

UNCRC (2021) General Comment No. 25 on the rights of the child in relation to the digital environment

non-discrimination
(article 2 UNCRC)

best interests
(article 3 UNCRC)

freedom of expression
(article 13 UNCRC)

freedom of thought
(article 14 UNCRC)

right to privacy
(article 16 UNCRC)

access to diverse
information + protection
against harmful content
(article 17 UNCRC)

right to play
(article 31 UNCRC)

right to protection from
commercial exploitation
(article 32 UNCRC)

life & development
(article 6 UNCRC)

right to be heard
(article 12 UNCRC)

Leisure time spent in the digital environment may expose children to **risks of harm**, for example, through **opaque or misleading advertising or highly persuasive or gambling-like design features**.

By introducing or using data protection, privacy-by-design and safety-by-design approaches and other regulatory measures, States parties should ensure that businesses do **not** target children using those or other techniques designed to prioritize commercial interests over those of the child.



States parties should **review, adopt and update national legislation** in line with international human rights standards, to ensure that the digital environment is compatible with the rights set out in the Convention and the Optional Protocols thereto. Legislation should remain relevant, in the context of **technological advances and emerging practices**.

Businesses should **respect** children's rights and prevent and remedy abuse of their rights in relation to the digital environment.

States parties have the **obligation to ensure** that **businesses** meet those responsibilities.



Children and young people think that EU policy-makers should exercise pressure on industry to provide safe, child-appropriate and age-appropriate services and platforms and to ensure that children's voices are heard. They suggested banning sexual or violent content, or restricting access to certain content such as gambling, advertisements and spam.



<https://www.betterinternetforkids.eu>

General Data
Protection Regulation

Audiovisual Media
Services Directive

Digital Services Act &
Digital Markets Act

Proposal for an AI Act

Proposal for a
Regulation laying
down rules to prevent
and combat child
sexual abuse

Proposal for a
Directive on combating
violence against
women and domestic
violence

Better Internet for
Kids+ Strategy

Age-Appropriate
Design Code
(announced)

Commission Notice
UCPD

2020 New Consumer Agenda

Children and minors are particularly exposed to [misleading or aggressive](#) commercial practices online.

UCPD Commission Notice

The Directive has a broad scope of application as it covers the totality of business-to-consumer transactions, [whether offline or online](#). It is technology-neutral and applies regardless of the channel, medium or device used to implement a business-to-consumer commercial practice. It applies to [online intermediaries, including social media, online marketplaces and app stores, search engines, comparison tools and various other traders operating in the digital sector](#).

Point No 28 of Annex I [prohibits direct exhortations to children](#) in commercial communications -> Targeted advertising practices that focus on children as the target group therefore cannot contain any direct exhortations to buy the advertised products under the UCPD.

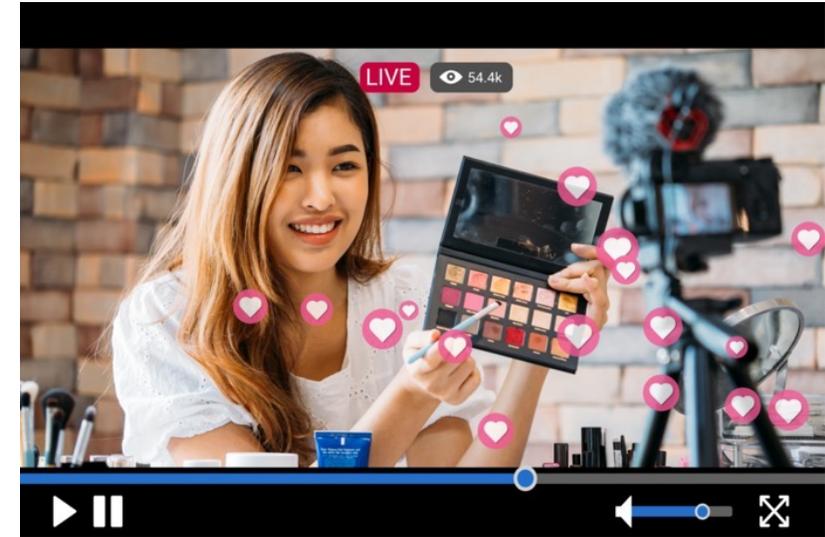
Focus on

- Influencer marketing
- Lootboxes
- Dark patterns

- what? risks for children?
- which legal frameworks?

Influencer marketing

- User-generated content, often engaging and interactive (esp. video)
- Influencers are perceived as relatable, accessible and credible
 - Ideal to influence (consumption) behaviour
- “Monetizing eyeballs”: controversial content generates views & revenue
 - E.g. glamourizing gambling, drug use, smoking or alcohol
 - Even more problematic in light of young audiences
- Revenue from brands, platforms, audiences and own business ventures

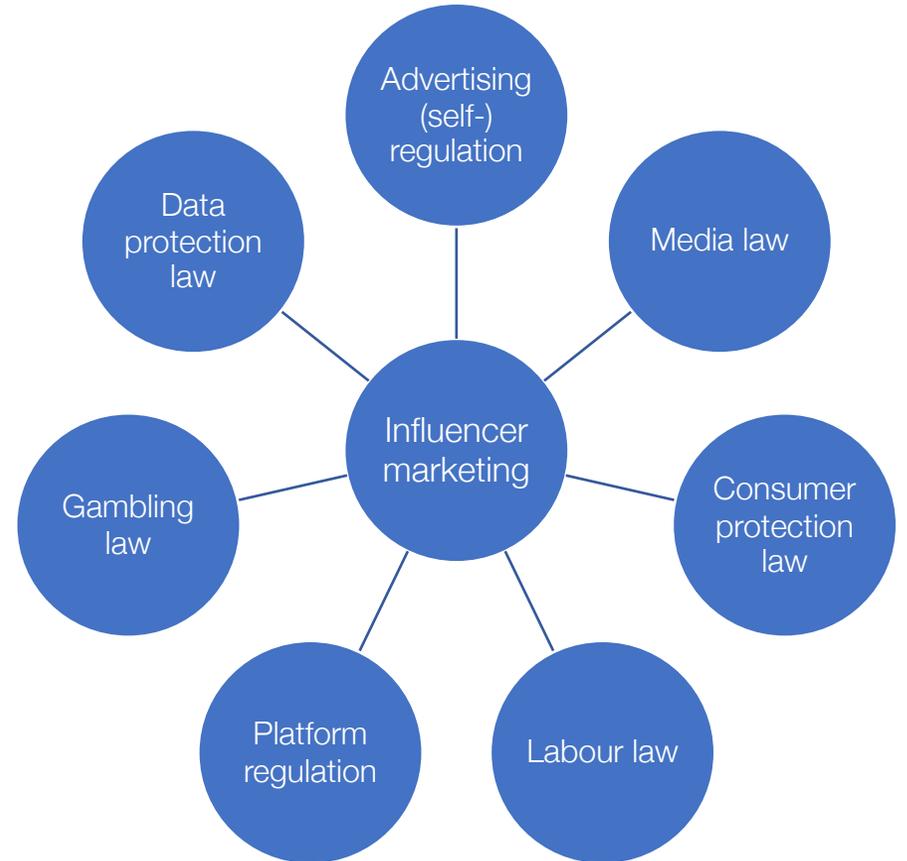


Picture: iStock

Influencer marketing

UCPD Commission Notice

Moreover, given that the relationship that the **influencer** builds with its audience is often based on **trust and a personal connection**, their behaviour could in some cases amount to an **aggressive commercial practice** through the use of undue influence, prohibited by Articles 8-9. This is particularly relevant when the main target audience of an influencer includes vulnerable consumers, such as **children and young people**. Furthermore, point No 28 of Annex I prohibits **direct exhortations towards children** in all circumstances.



Loot boxes

= 'mystery boxes' which contain randomised items and which are accessed through gameplay, or paid for with real-world money



- 51,6% of respondents already opened a free lootbox
- Around 25% of respondents sometimes pays for a lootbox
- 14,8% of respondents tries to regain money by selling lootbox items

Source: https://www.gameable.info/_files/ugd/7f91ff_c197ace0298e44ff8dca0fb124e36b78.pdf



Picture: iStock



Loot boxes

UCPD Commission Notice

The presence of [paid random content](#) (e.g. loot boxes, card packs, prize wheels) should be **clearly disclosed to the consumer, including an explanation of the probabilities of receiving a random item**. For example, loot/mystery boxes are in-game content that generally include random items that have relevance in the game (e.g. weapons, skins, game currency, advancement options). The sale of loot boxes in games must comply with the **information obligations** under the CRD and UCPD concerning the price and main characteristics of the product.



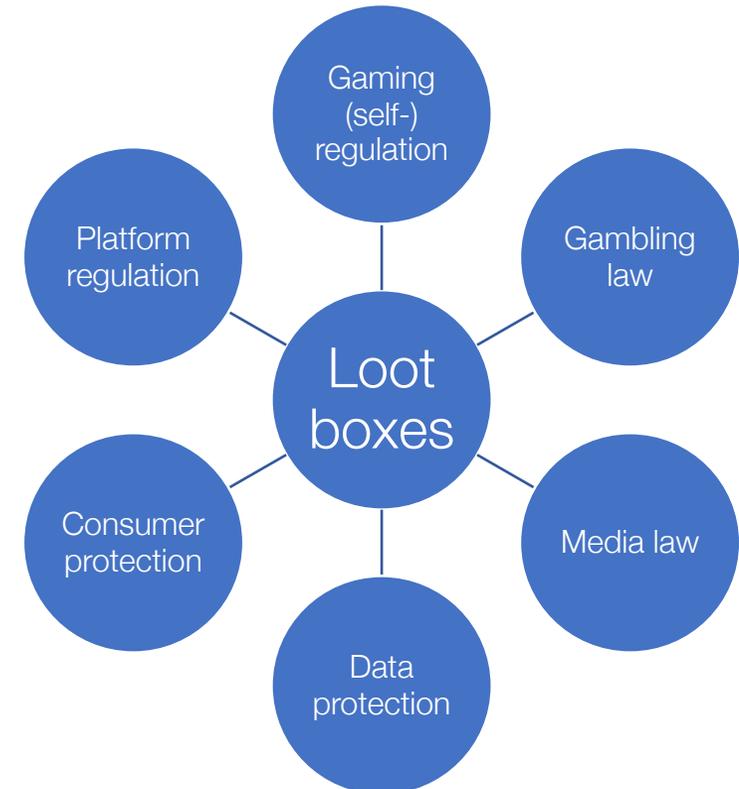
FIFA 22

EA Swiss Sarl

Football simulation game in which players can choose from over 600 real teams across various national and international leagues.



In-game Purchases (includes random items)



Dark patterns

The term ‘**dark pattern**’ is used to refer to techniques, incorporated in the design or structure of websites, platforms or apps, that make you do things or take decisions that you did not mean to.

Dark patterns can be

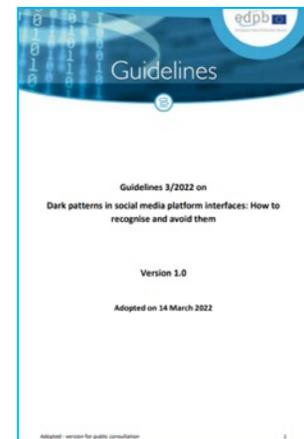
- personalised (based on collection of personal data), or
- general (relying on knowledge of human behaviour; e.g. anchoring, default effect, framing effect, scarcity bias, sunk cost fallacy)

- visually designing buttons so as to make the desired option to be more visible or attractive (colours, prominence)
- using trick questions and ambiguous language (e.g. double negatives)
- using emotion(al language) to discourage certain choices, make the user feel guilty (peer pressure)
- sense of urgency (encouraging FOMO or faster action)

According to the mystery shopping exercise, 97% of the most popular websites and apps used by EU consumers deployed at least one dark pattern.

European Commission, Directorate-General for Justice and Consumers, Lupiáñez-Villanueva, F., Boluda, A., Bogliacino, F., et al., Behavioural study on unfair commercial practices in the digital environment : dark patterns and manipulative personalisation : final report, Publications Office of the European Union, 2022, <https://data.europa.eu/doi/10.2838/859030>

Dark patterns



https://edpb.europa.eu/system/files/2022-03/edpb_03-2022_guidelines_on_dark_patterns_in_social_media_platform_interfaces_en.pdf



https://www.beuc.eu/sites/default/files/publications/beuc-x-2022-013_dark_patterns_paper.pdf

Key take-aways

- ⇒ address risks by means of **a variety of** - existing & proposed – instruments
- ⇒ towards a legal framework with **stronger obligations** for platforms/companies
 - ⇒ Age-Appropriate Design Code?
- ⇒ **future-proof?** e.g. gaming environments merging with AV content, livestreaming of gaming & gambling
- ⇒ **enforcement?**
 - ⇒ by national (Irish?) regulators
 - ⇒ dissuasive sanctions
- ⇒ **cooperation** between different authorities (data protection authorities, consumer protection authorities, media regulators, gambling authorities, ...)
- ⇒ still **uncertainty** regarding the application and interplay of certain instruments

Key take-aways

- ⇒ **best interests** of the child!
 - ⇒ ‘by design’ approaches
 - ⇒ precautionary principle
 - ⇒ research needed!
- ⇒ Child Rights Impact Assessments
- ⇒ **seek children’s views!**
- ⇒ put effort into maximising the **positive** potential of the digital environment

Children are agents, actors, citizens, not just victims in need of protection.

Sonia Livingstone (2022) Reflecting on Youth Mental Health and Tech Regulation in Anticipation of the Metaverse, *The Children’s Media Yearbook 2022*,
<https://www.thechildrensmediafoundation.org/wp-content/uploads/2022/06/The-Childrens-Media-Yearbook-2022.pdf>

Thank you!

Prof. dr. Eva Lievens

Law & Technology
Ghent University



eva.lievens@ugent.be



@evalieve

www.ugent.be

<https://www.ugent.be/re/mpor/law-technology/en>

The logo for 'Gameable' features the word 'Gameable' in a dark blue, rounded font. The letter 'e' is replaced by a stylized, light blue outline of a game controller, with a joystick on the left and buttons on the right.

<https://www.gameable.info/>

Gam(e)(a)ble: Interdisciplinary research on the blurring lines between gaming and gambling among teenagers

See also: Pieterjan Declerck and Nadia Feci (2022). 'Mapping and analysis of the current regulatory framework on gambling(-like) elements in video games – a report in the framework of the 'Gam(e)(a)ble' research project', https://www.gameable.info/_files/ugd/7f91ff_0b51d9c313db43729fe6150ec671219a.pdf