OECDpublishing

PUTTING PEOPLE FIRST IN DIGITAL TRANSFORMATION

BACKGROUND PAPER FOR THE

CDEP MINISTERIAL MEETING

OECD DIGITAL ECONOMY PAPERS

November 2022 **No. 339**

OECD
BETTER POLICIES FOR BETTER LIVES

Foreword

This paper looks at how digital transformation impacts us as individuals, be it as citizens, consumers, or workers. It outlines the policy landscape, and describes the international, multi-stakeholder and nuanced efforts needed to strike a balance between different rights, interests and values.

This paper provides background to support the discussions on Theme 3: Putting People First of the Ministerial meeting of the Committee on Digital Economy Policy, taking place on 14-15 December 2022 in Gran Canaria, Spain. It informs the sessions on 'Rights in the digital age – building solid evidence (workshop)', 'Creating a safer online environment (workshop)' and 'Empowering consumers in a digital world' of the Ministerial meeting.

This paper was written by Nora Beauvais, Giuseppe Bianco, Kosuke Kizawa, Nicholas McSpedden-Brown and Lisa Robinson, under the supervision of Audrey Plonk, Head of the OECD Digital Economy Policy Division. It benefitted from the inputs of Brigitte Acoca, Gallia Daor, Clarisse Girot, Molly Lesher, Adam Mollerup, Vincenzo Spiezia, Verena Weber and Jeremy West, as well as from Angela Gosmann, Sebastian Ordelheide and Misha Pinkhasov, who provided editorial support. The Ministerial meeting and related work were generously supported by the Government of Spain.

This paper was approved and declassified by written procedure by the Committee on Digital Economy Policy on 26 October 2022 and prepared for publication by the OECD Secretariat.

Note to Delegations:

This document is also available on O.N.E under the reference code:

DSTI/CDEP(2022)13/FINAL

This document, as well as any data and any map included herein, are without prejudice to the status of or sovereignty over any territory, to the delimitation of international frontiers and boundaries and to the name of any territory, city or area.

Table of contents

Figures

Boxes

Executive summary

Digital transformation offers a multitude of social and economic opportunities for people as citizens, consumers and workers. Digital technologies transform billions of lives, offering new spaces and tools to communicate, work, consume, participate in the economy and the public debate, and exercise rights and enjoy liberties. Creating an empowering and safe online environment is key to putting people first in digital transformation.

To consumers, digital technologies offer tailored products and services, ease of access to marketplaces, expanded choices and competitive prices, and connected homes. However, people risk falling victim to online scams and frauds, buying unsafe products, being deceived, exploited, or discriminated against.

As workers, people have access to new and more flexible opportunities, platform-mediated work and practical tools. However, they might suffer difficult working conditions, decentralised management, or algorithmic bias.

For individuals, digital technologies unlock numerous possibilities to build relationships, relax, learn, or participate in government. However, people might encounter illegal and harmful content online, have their privacy violated, or suffer from discrimination, inequality or security breaches.

The policy landscape of the digital environment requires international, multistakeholder and nuanced efforts to strike a balance between rights, interests and values. Policy makers and enforcement authorities increasingly focus on protection, empowerment, safety and rights, but they need tools to support these efforts. Soft measures are essential to complement regulation and enforcement, and can include voluntary pledges, ethical standards, by-design approaches, technical measures and education and awareness campaigns. Laws and policies should reflect the interdependencies of the digital environment and be based on evidence to bridge policy gaps and provide responses that are fit-for-purpose.

Putting people first is more than a slogan or aspiration – it reflects the core goals of the digital age.

Putting people first in digital transformation: Background paper for the CDEP Ministerial meeting

Digital technologies are intertwined with people's lives…

Digital transformation offers societal benefits for people as citizens, consumers and workers. Technological advances and new business models have reshaped the everyday lives of billions of people, creating new public spheres and new markets for goods and services. Chatting, sharing content, shopping online, using connected objects and paying with smart devices open new possibilities for people to communicate, work, consume, learn and create, participate in democracy and the economy, and exercise and enjoy their rights in the digital age.

What does this mean in practice? Let's take the family of Antonio, a 45-year-old schoolteacher and father of two. He and his partner Yoko connect online with their relatives and friends around the world whenever they want. In their family chat, they exchange news, memes and cat videos and pictures of their kids and holidays. Antonio thinks this helps keep the family together, especially since his parents live so far away. Yoko, a keen environmentalist, also often turns to the Internet to learn new information and enjoys discussing environmental issues on social media, where she shares articles and ideas in online communities. Through one of these groups, she recently reconnected with former friends from high school with whom she had lost touch.

Antonio is not an avid social-media user and does not always understand the appeal of vlogs, tweets, or streams. However, smartphones make it easier to keep track of the kids, Tom, 14, and Ana, 11, who do use social media, though Antonio and Yoko were wary about Ana having an account at such a young age. The kids seem to spend hours glued to their screens – too many if you ask Antonio. Tom spends much of his time playing video games with friends he made online, some of whom he has not met in real life. He also loves to draw comics on his tablet. As for Ana, she either watches cartoons or chats with friends on social media – or both at the same time. Antonio says his kids have made outstanding progress in French thanks to a new interactive app. They have access to so many educational resources, knowledge and information! During the lockdowns, like many teachers, Antonio made use of e-learning platforms, through which he gained a better understanding of his students' learning needs. One of his students did not have Internet at home, and Antonio, his colleagues and other students collected money to get the student access to a data-connected tablet.

Digital transformation has unlocked flexible employment opportunities for the family. Yoko's brother Ken drove for a ride-share service to earn extra money during university. This let Ken, a single father, choose when and where to work around his study schedule. After university, Ken continued working as a driver from time to time to increase his earnings. Ken drove for multiple platforms and, while he was not aware of the technology behind it, could ask for his ratings on one platform to be transferred to the other ('reputational data portability'), which meant he did not feel confined to the one platform for fear of losing his high rating.

Ken is one of many people who might have struggled to make ends meet but found an income opportunity through platform-mediated work, defined as "any productive activity performed by persons to produce goods or provide services carried out through or on a digital platform" (OECD, 2022[1]). This might comprise a worker's main job or occasional secondary work to supplement income (e.g. for students, people who recently lost their jobs, or new retirees).

…but people can be vulnerable to their drawbacks.

However, it was not perfect. It was Ken's responsibility to maintain his car and make sure he had the necessary training for his licence. When COVID-19 hit, he started worrying about his health because he had contact with so many people and, if he were to get sick, he would not be able to work and get paid. Ken also found it hard to budget. He never knew how much he would earn, and sometimes a passenger would refuse or dispute a payment, meaning he lost money. Once, a platform deactivated his account and Ken did not know beforehand that this was going to happen or why. The platforms had no simple dispute resolution mechanism, and Ken felt like he had little power to raise these problems.

Ken saw his ranking decrease slightly after he took several days sick leave when he caught COVID-19. Algorithmic systems that power platform-mediated work can be prone to discrimination and bias. Other similar cases have been reported: in 2020, a reputational-ranking algorithm used by an on-demand food delivery platform in Italy penalised workers absent for either trivial or legitimate reasons (e.g. strikes, sick leave). It was thus deemed in breach of Italian law (Tribunal of Bologna, 2020[2]).

Digital technologies empower citizens…

Digital technologies and data transform citizens' relationship with government, empowering them with new means to participate in democracy and civil society. Digital government allows for openness and public engagement to bring people into the design, development, delivery and monitoring of public policies and services. In line with this, countries are taking a mobile-first approach to digital government. Digital technologies are also transforming the ways democratic processes and institutions function, opening opportunities (e.g. e-voting, e-counting), but posing challenges in terms of privacy, equality and security. To address these, governments often work with private-sector partners on measures to build trust.

The advent of electronic signatures and e-IDs help Antonio and Yoko save a lot of time. Their son, Tom, uses digital technologies to develop his civic identity and engage in political issues. He and many of his friends are part of an online, environmental action youth group. This is one of many ways digital transformation facilitates children's civic engagement, amplifies their voices and enables them to advocate for rights and interests, individually and collectively. At the same time, the concentration of information on citizens' activities in a centralised scheme could give rise to risks like unwarranted intrusion (ICO, 2021[3]).

… and enable tailored commercial services…

Antonio makes the most of online commerce by posting wooden tables that he refurbishes for sale to an online marketplace. He also makes most of his purchases online, following the trend (accelerated by the COVID-19 pandemic) of consumers in OECD countries shopping online: 64% in 2020, up from 36% in 2010. After entering keywords into algorithmically tuned search engines on his smartphone, he compares dozens of offers for a vast array of products, often in online marketplaces, where he reads detailed consumer reviews. Digital comparison tools, personalised ads and recommendations help him pinpoint what he needs. Sometimes he shares ideas with his wheelchair-bound younger sister, María, who can order and receive products entirely independently with a flick of her finger. They make these transactions easily, using digital banking and payments. Antonio felt lucky to have easy access to the global marketplace during the lockdowns driven by COVID-19, during which he purchased online even more, as he was aware that some people were excluded due to lack of access.

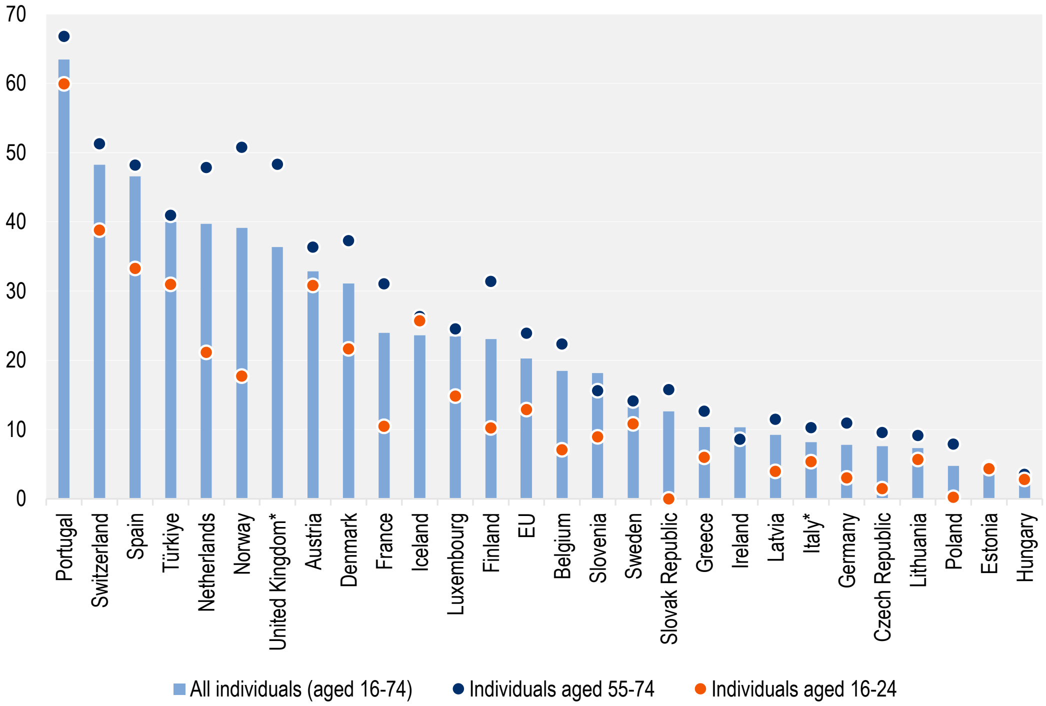
When Yoko arrives home after work, she speaks to her digital assistant, powered by artificial intelligence (AI), which turns her Internet-connected heating and lights on, streams music throughout the house, updates her on tomorrow's weather and books a restaurant for dinner. With the data it collects and continuous remote updates, it learned to adapt the household's energy consumption to the family's needs. It also suggests more tailored offers, as does another app based on their transaction data.

…but concerns over online business practices abound.

However, e-commerce and digital consumer products have not always been helpful, and the family had some harmful experiences online. During the COVID-19 crisis, Antonio's order of hand sanitiser from a genuine-looking online retailer never arrived: it turned out to be a fake website that used AI-generated reviews and stolen logos to appear legitimate. Yoko ordered face masks that turned out to be faulty and could have injured the children. In addition, she came across charitable appeals to help victims of the virus, which turned out to not be legitimate, and she learned of the risks stemming from phishing and online financial fraud. These experiences led Antonio and Yoko to be more careful when purchasing online and sharing their financial and personal information. They are not alone in these concerns, with OECD statistics showing that 22.5% of Internet users do not buy online due to payment security and privacy concerns (Figure 1) (OECD, n.d.[4]).

Figure 1. Share of Internet users not buying online due to payment security concerns

% of Internet users who did not buy online in the last 3 months



Note: Internet users who did not order goods or services over the Internet in the last 3 months include those who have never made online purchases. The latest data refer to a recall period of 3 months prior to being surveyed, though some countries use different periods and recall periods may vary over time. In 2021, Eurostat changed the recall period from the previous 12 months prior to being surveyed to the previous 3 months. For more information about definitions, data quality, breaks in series, etc., please visit the underlying data source(s).
Source: The OECD *Going Digital Toolkit*, based on the Eurostat Digital Economy and Society Statistics Comprehensive Database.

E-commerce raises a wide range of concerns for people. A 2021 OECD survey across 13 countries showed that 50% of online consumers faced at least one problem in e-commerce in the 12 months preceding the survey. Considering only their most serious problem, around 25% were related to the COVID-19 crisis (in relation to which scams were frequent), and total costs to consumers across OECD countries were estimated at over USD 22 billion in 2020 (OECD, 2022[5]). Preliminary data from a 2021 OECD online product-safety sweep across 21 jurisdictions suggest that average rates of non-compliance with bans/product recalls, labelling requirements and safety standards have not improved since a 2015 sweep for consumer products in seven categories (toys/games, household electrical, household non-electrical, sporting/recreation, apparel, children/infant, portable technology) (OECD, forthcoming[6]; OECD, 2016[7]).

Certain business practices might further undermine trust…

Yoko recently signed up for an online service that teaches children to play musical instruments. She was not entirely satisfied but struggled to cancel it due to a combination of hidden information, trick questions, lengthy cancellation steps and emotive language coaxing her to stay. After a very short trial period, she was subscribed and billed for a whole year's subscription by default. Yoko had fallen victim to several "dark commercial patterns" (hereafter "dark patterns") – business practices employing elements of digital-choice architecture, in particular in online user interfaces, that subvert or impair consumer autonomy, decision-making or choice. Like many consumers, Yoko was unaware of how common they are, although she had heard about action taken by the US Federal Trade Commission (FTC) against an online business for automatic renewal of consumers' subscriptions without consent, which led to USD 9.7 million in refunds to consumers affected by the practice in 2021 (FTC, 2021[8]).

In 2022, the OECD found that dark patterns are prevalent on e-commerce websites, apps (including those of major online platforms and marketplaces), and in cookie consent notices, search engines and games (OECD, 2022[9]). One study identified at least one dark pattern in 95% of 240 popular apps (Di Geronimo et al., 2020[10]). They often deceive, coerce or manipulate consumers, and are likely to cause direct or indirect consumer detriment, though this may be difficult or impossible to measure. There is evidence of their effectiveness in influencing consumer decision-making and possible harms in terms of financial loss, privacy harms, psychological detriment, weaker or distorted competition and loss of consumer trust. Some consumers, such as less educated, low-income consumers, or children, might be disproportionately harmed.

Mindful of Yoko's experience, Antonio worries that his children might be susceptible to dark patterns. In video games, Tom increasingly spends his pocket money on purchases to obtain randomised items ("loot boxes"), which appear to use the same deceptive design and aggressive marketing techniques that Yoko fell victim to. Around 60% of the top games on the Google Play and Apple stores reportedly contain loot boxes (Zendle et al., 2020[11]) and 44% of 11-16-year-olds in the UK who were aware of loot boxes had spent money on them (Gambling Commission, 2019[12]). Disturbingly, children also rarely seem to identify advertising and endorsements in games and social media (OECD, 2021[13]).

…which makes people wary of online interaction in general.

Occasionally, Antonio thinks about the data footprint that his family's always-online presence leaves. He acknowledges he does not really know what his family's data are ultimately used for, especially as no one in the family ever reads any of the cookie consent notices, terms-of-service or privacy policies, finding that they are too long and often feeling that they must agree to them anyway. The children's lack of awareness of the value their data can hold for businesses might indeed put them at greater risk of having their privacy rights breached.

Antonio sometimes worries about whether having so much personal data exposed to businesses' algorithmic profiling could make them more vulnerable to exploitation or discrimination, though he is not sure how well-founded these fears are. What if businesses could determine their individual emotional states, biases, or health issues at key moments and target them with manipulative ads or make them pay more than others? Could algorithms learning with historical data replicate or exacerbate the marginalisation his sister, María, experiences as a person with a disability? Antonio also heard that algorithms and AI can have disproportionate impacts on people along racial or ethnic lines and other protected characteristics.

Online social interactions can also pose dangers...

Digital transformation has enabled faster, cheaper and wider dissemination of harmful content. At school, just a few weeks ago, Antonio and Yoko's son, Tom, attended a prevention course on cyberbullying. He learned that digital technologies facilitate the spread and amplification of cyberbullying, and that it is often associated with high levels of stress social difficulties, depression, anxiety, self-harm and suicide. Other types of harmful content, such as propaganda and disinformation, can pose threats to democracy with wide-reaching implications. Antonio's family still remembers a scandal, when a political consulting firm harvested and sold the data of 50 million users of a social network without their consent, to influence voters (ICO, 2018[14]). The terms "echo chambers" and "filter bubbles" have been used to describe like-minded communities online, with limited exposure to different viewpoints. Sometimes reinforced by algorithms, these can contribute to the proliferation of false and misleading information, intellectual isolation, exacerbated bias and the polarisation of ideological positions. This trend extends to content that is illegal. For instance, Yoko often heard in news reports about perpetrators of terror attacks who had been radicalised online or livestreamed the attack.

Although she knew she was not allowed to, Antonio and Yoko's 11-year-old daughter, Ana, installed a social media app on her phone that everyone else in her class was using. Last summer, she received an invitation through that app from a stranger to chat. Because they had friends in common, she accepted and they started chatting, but he suddenly sent her several violent and pornographic pictures. He also started asking her to send pictures of herself. She blocked him right away, but she was too scared and shocked to tell her parents what had happened. They could tell something was wrong, however, as she was highly distressed.

The scale of child sexual exploitation and abuse (CSEA) online is expanding at a horrifying rate. Victims are predominantly girls, though boys are also affected; victims are mostly aged 3-13, though images often depict children 0-2 years old. An increase has also been seen in "sextortion", where predators demand sexual favours, money, or other benefits from a child under threat of sharing their self-generated content (WeProtect Global Alliance, 2021[15]).

…while protective measures carry risks of their own.

Yoko's research found that existing and emerging digital technologies and algorithms can detect and take remedial action against harmful and/or illegal content and practices. Examples include tools to detect and remove terrorist and violent-extremist content online using cross-company shared databases or tooling, or that automatically identify harmful commercial practices online. However, Yoko's research also taught her that algorithmic content detection using AI can come with limitations and problems of its own, given that such tools can be inaccurate, biased, discriminatory by design, and might facilitate mass censorship and surveillance by companies (FTC, 2022[16]) or even governments.

Mass surveillance technologies can compromise freedom of expression and privacy, but also physical safety and ultimately the right to life. Indeed, in certain countries, the use of surveillance technologies has been linked to arrests, intimidation, and the killing of journalists and human rights activists. They can also cause fear and lead people (including journalists, advocates and activists) to self-censor, threatening freedom of expression and people's capacity to access information. Surveillance technologies can further compound the physical and psychological impacts of gender-based and intimate-partner violence.

Yoko read in the news that the FTC took action against a company selling "stalker-ware" apps, which can be installed surreptitiously on devices and used to monitor photos, text messages, web histories, GPS locations and other personal information without the device owner's knowledge (FTC, 2021[17]).

Policies need to put people first

Antonio, Yoko, Tom, Ana, Ken and María are fictional, but the challenges described above are real for millions of people worldwide. Given the multitude of benefits and risks that the digital environment brings, it is essential that people's economic welfare, psychological and physical safety, and well-being, are at the forefront of policymaking. This does not imply a purely protectionist approach, but rather one that meets the twin priorities of protection and empowerment, and that maximises benefits while mitigating risks. While further action is needed, the OECD has long been at the forefront of these issues (Box 1).

Box 1. OECD work to help put people first in digital transformation

Privacy

- OECD Privacy Guidelines
- Recommendation on Cross-border Co-operation in the Enforcement of Laws Protecting Privacy

Children in the digital environment

- OECD Recommendation on Children in the Digital Environment
- Guideline for digital service providers

Transparency Reporting

- Benchmarking reports 2020; 2021; and 2022
- Voluntary Transparency Reporting Framework (VTRF)

Consumers

- Guidelines for Protecting Consumers from Fraudulent and Deceptive Commercial Practices across Borders
- Consumer Protection in E-commerce
- Consumer Product Safety

A multilateral and nuanced policy effort

Safeguarding the well-being of people in their role as citizens, workers and consumers, and ensuring that their rights are protected and respected, requires coordinated, evidence-based policy approaches.

The challenges in addressing the harmful effects of false and/or misleading content – including misinformation, disinformation, propaganda, contextual deception and satire – that circulate widely and quickly online illustrates this complexity. This makes a balance with freedom of expression and access to reliable information about global challenges like climate change complicated in the digital age. When governments or firms overreach in their efforts to remove harmful or misleading content, they can improperly restrict speech. The right to freedom of expression, and a free and independent press are indispensable for the healthy functioning of democratic societies (OECD, 2022[18]). But care should be taken to balance freedom of expression with other rights, such as to health and privacy.

Privacy and data protection are often at the centre of debates on balancing competing rights and interests. How can consumers reap the benefits of personalised advertising and content without compromising the protection of their data? End-to-end encryption is often viewed as essential for protecting privacy, but when combating CSEA, for example, it can be seen as providing an unmonitored playground for malicious actors. This dilemma requires collaboration between policy makers, civil society, technology and privacy experts, law enforcement and child protection specialists.

There can also be a need to think more critically about how we uphold certain rights. For example, still common assumptions that anonymised or "de-identified" data have no privacy implications are increasingly questioned. De-identification might guard against the disclosure of an individual's identity and provide privacy protection, but it does not protect against the attribution of traits or characteristics of groups to which they may belong. This raises questions regarding the collective rights of groups (such as indigenous people), including their capacity for self-determination and to assert sovereignty over their data to address systemic disadvantage (OECD, 2022[19]). It has been argued that people should have visibility or transparency regarding what is done with their personal data after such data are de-identified, and they should be given the information to assess whether such use is in line with their values (FNIGC[20]). Transparency solutions are mostly insufficient in isolation, and their merits will often be limited for individuals, given the time and complexity involved in monitoring how their personal information has been used across different technologies.

It is important that policy makers ensure they avoid harmful unintended consequences, e.g. creating new social problems when regulating existing ones. Legal responses to sexting provide a prime example. Children who engage in sexting might be self-generating material that is legally classified as CSEA, and many children have been captured in a criminal justice response, including by being prosecuted or placed on a mandatory child sex-offence register, which can have life-long negative impacts. The OECD Recommendation on Children in the Digital Environment seeks to address this, recommending that measures to protect children in the digital environment be proportionate, not unduly punitive, and, where appropriate, educational and therapeutic in the first instance (OECD, 2021[21]).

Consumer protection, empowerment, safety and rights at the fore of policy and enforcement

Laws related to combatting many of these emerging risks already exist. Many jurisdictions have privacy and data protection laws reflecting common international standards such as the OECD Privacy Guidelines, which set out basic principles for promoting privacy. In many jurisdictions, consumer laws, which reflect key principles in the 2016 OECD Recommendation on Consumer Protection in E-Commerce (OECD, 2016[22]) and the 2020 OECD Recommendation on Consumer Product Safety (OECD, 2020[23]), include prohibitions on misleading, deceptive, fraudulent, unfair and other harmful commercial practices, and on placing unsafe products on the market (OECD, forthcoming[24]; OECD, 2022[9]). Many provide special protections for vulnerable consumers, such as children (OECD, forthcoming[24]). Accordingly, consumer and data protection authorities can (and do) respond to many concerns. Likewise, many countries follow the OECD Recommendation on High-Level Principles on Financial Consumer Protection (OECD, 2012[25]) to establish or enhance their frameworks in this area and address the impact, opportunities and risks of digitalisation.

However, there is consensus that more comprehensive enforcement is needed, and existing regulation is not enough in many cases. This is in part because the digital environment is so different from the offline world; it has ubiquity, great speed and scale and knows no borders. In addition, data and content can be replicated at no or low cost and shared or used in algorithms.

Until recently, many areas of the digital environment relied on self-regulation by private entities that often benefited from liability exemptions. High-level international fora and policy makers are increasingly considering how to protect the economic welfare, privacy, safety and well-being of us all in the digital transformation by implementing or proposing new regulations.

Policy makers stress the role of online businesses and platforms in solutions to online harms. This is recognised at the OECD, and at G7 and G20 level.[1] Often these calls emphasise shared responsibility and the need for a multistakeholder approach. For example, the OECD Recommendation on Consumer Protection in E-commerce emphasises businesses' shared responsibility for promoting consumer welfare and enhancing consumer trust, calling on them to pay due regard to consumers' interests (OECD, 2016[22]).

At the same time, policy makers are proposing obligations on online businesses – particularly platforms, including marketplaces – to protect consumers and prohibit harmful practices. Several new or proposed laws seek to ban dark patterns, constrain targeted advertising or place obligations on online marketplaces to mitigate the sale of unsafe products. Other proposed laws seek to address harmful practices or consumer products that incorporate AI, such as prohibiting subliminal techniques or those that exploit vulnerabilities to materially distort behaviour (OECD, 2022[9]).[2] Other measures seek to empower consumers to make more informed decisions online, including through more effective disclosures (OECD, 2022[26]).

Specific attention has been given to the transparency and accountability practices of online platforms, especially larger ones. Ever more jurisdictions impose transparency requirements for online platforms, including on content moderation policies and actions, and sanctions for non-compliance. Requirements include reports on detection methods (e.g. human review, automated technologies, trusted notifiers) and actioning methods (e.g. content removal or blocking, warning labels, suspension or removal of account), and on complaint mechanisms, dispute settlements and risk assessments. Many of these measures are part of laws that aim to address online safety more broadly.[3] These too often centre on the activities of online platforms and propose requirements to make it easier to report illegal or harmful content, to have it removed, and impose sanctions should requirements not be respected. This is also true for the use of personal data. An Australian Competition and Consumer Commission inquiry found a lack of transparency on digital platforms and of informed consumer choices over the collection and use of data, and the need to strengthen protections in the privacy law (ACCC, 2019[27]).

Combatting harms against children and gender-based violence is a prominent issue and many proposals include measures to address gender-based or intimate-partner violence,[4] or children's vulnerabilities. Measures for children include the proposed EU Regulation laying down rules to prevent and combat child sexual abuse (EC, 2022[28]) or require that age-appropriate privacy-by-design be implemented specifically for children.

Attention is also being given to the interests of workers online. According to the OECD, governments should ensure that all workers have access to adequate rights and protections, regardless of their employment status or contract type, and should guarantee a level playing-field by preventing some firms from gaining an unfair competitive advantage (OECD, 2019[29]). The proposed EU directive for improving working conditions on platforms sets out protections related to whether a platform should be considered an employer (as opposed to considering the workers self-employed). This will provide workers with benefits like paid leave, pension rights and minimum wage requirements (EC, 2022[30]). Policy makers and privacy regulators are turning their attention to data portability, which can support gig workers maintaining their reputational data across platforms.

These issues are increasingly examined in the context of rights. Does digital transformation change expectations of how governments uphold and protect rights? Do digital technologies complicate the balancing of competing rights? While some countries look at specific individual rights, such as to protection of personal data or to Internet access (Conseil d'État, 2016[31]), others consider the question more holistically, launching broad initiatives to protect rights in the digital age and ensure a human-centric digital transformation. In 2021, the Spanish government adopted the Charter of Digital Rights (Government of Spain, 2021[32]); in 2022, the European Commission proposed a Declaration on Digital Rights and

Principles to enshrine them in the digital transformation (EC, 2022[33]); and Korea expects to introduce a Bill of Digital Rights in 2023 (Ministry of Science and ICT, Republic of Korea, 2022[34]).

Some jurisdictions are exploring new rights in specific domains, such as algorithmic transparency and accountability in AI decision making, while others prioritise protecting rights online and offline the same way. At the international level, the issue of upholding rights online is advanced when it comes to children. In 2018, the Council of Europe developed Guidelines to respect, protect and fulfil the rights of the child in the digital environment (CoE, 2018[35]); and in 2021, the Committee on the Rights of the Child issued a General Comment on children's rights in the digital environment (CRC, 2021[36]). With regard to the responsibility of businesses to respect rights in the digital environment, the UN Office of the High Commissioner for Human Rights' B-Tech Project provides guidance and resources for implementing the United Nations Guiding Principles on Business and Human rights in the technology space (OHCHR, n.d.[37]).

Laws and policies interoperable across borders and issues

Policy makers and regulators should keep in mind that the digital environment crosses traditional boundaries and has significant interdependencies. Examples of fragmented policy responses abound. Responsibility for meeting children's needs online is often left to ministries that address this in the offline space (OECD, 2020[38]), even though many issues such as sexting and cyberbullying require a coordinated response from justice, health and education (at a minimum), and consideration of the impacts on children's privacy rights. Similarly, fragmented transparency, reporting and accountability to address violent and extremist content could be costly and inefficient. Multinational businesses might have to issue several versions of transparency reports, governments could individually replicate legislative costs, and stakeholders would likely need to search for reports in different places. To address this, in May 2022, the OECD launched the Voluntary Transparency Reporting Framework (OECD, 2022[39]), a standardised, international hub that any online content-sharing service can use, regardless of its size or business model.

Often, the same issue engages several policy areas simultaneously, driving a need for regulatory co-operation. Dark patterns, exploitative personalisation practices and algorithmic bias can involve consumer, privacy, competition, artificial intelligence and anti-discrimination policies. The ubiquity of data across economic and social sectors means that privacy and data-protection laws must interoperate across regulatory areas such as competition and consumer authorities (OECD, 2022[40]), which deal with different questions. While privacy enforcement authorities might assess the data protection impacts of economic concentration, competition authorities must address whether the presence of personal information or privacy concerns changes competition analyses. It is important to understand to what extent authorities can co-operate and how their regulatory ecosystems can interoperate. Several countries have fora to enhance co-operation among digital regulators, including consumer, privacy, competition and communication regulators.

Instead of siloed and uncoordinated responses, governments and regulators should develop holistic approaches in consultation with civil society and business, foster synergies and co-operation between policy areas, avoid overlapping efforts and determine the best mechanism to address the issues. The OECD Recommendation for Agile Regulatory Governance to Harness Innovation calls on governments to lay the institutional foundations that enable co-operation and joint approaches within and across jurisdictions (OECD, 2021[41]). Further, policy coherence can help OECD countries achieve the Sustainable Development Goals, which are multi-dimensional and span many policy areas relevant to putting people at the forefront of digital transformation.

Cross-border co-operation is vital because online risks such as deceptive and fraudulent practices, privacy threats and unsafe products are transnational problems. But challenges persist. Enforcement bodies often lack the authority to fully engage in co-operation or can face practical challenges in working with their foreign counterparts. In 2021, the OECD released guidance for legislative action to give consumer authorities powers and tools to enforce consumer-protection laws domestically and co-operate across borders (OECD, 2021[42]). The new OECD Recommendation on International Regulatory Co-operation to Tackle Global Challenges helps governments and regulators transform governance and rulemaking processes – which focus inward – to realise the benefits of international co-operation (OECD, 2022[43]).

Evidence-based regulatory efforts

Setting policy priorities that maximise protections and enhance opportunities requires solid, up-to-date and reliable evidence to understand where policies work well and where they do not. For several challenges, including those faced by Yoko and Antonio's family, big gaps remain in the evidence base.

Dark patterns are one area that needs improved evidence to support policy and enforcement. This includes a need to understand the effects of certain dark patterns on consumer decision-making and the scale of consumer harms. Often, the need is not just for more or better evidence, but also for different types of evidence. According to the 2016 OECD Recommendation on Consumer Protection in E-commerce, incorporating behavioural insights is critical to bolstering the evidence base for consumer policymaking, including through empirical research like experimentation.

The evidence base for policymaking on privacy issues has been uneven too. Privacy enforcement authorities gather considerable data made public through annual reports, but not necessarily in a format suited to international comparison. A recurring source of concern are the growing gaps between privacy and data-protection laws globally, despite general alignment with the data-protection principles of the OECD Privacy Guidelines. These gaps might stem from differences in practical application of the principles or from similar rules being based on different rationales. However, as technology evolves, as data become more ubiquitous, and as more countries adopt privacy laws, new evidence is required to identify these gaps and assess whether the solutions remain relevant.

Likewise, there are significant gaps in the evidence needed to protect and empower children online. Policymaking for children in the digital environment is often reactive (e.g. to high-profile incidents) or based on partial evidence rather than driven by reliable and representative data. For example, while it is common to hear that too much 'screen time' is damaging to children's health and well-being, the evidence base for such concerns is lacking. Concerns about screen time also overlook that children are not a homogenous group, and that online vulnerabilities are influenced by their vulnerabilities offline (e.g. gender, socio-economic background). Moreover, screen time does not present a uniform risk and is not always damaging, as it depends on activities children engage in online. There is a difference between a teenager at risk of an eating disorder seeing unrealistic body images, and one finding a supportive community around a topic they care about. There is need for comprehensive, good quality, large-scale studies on the health and well-being effects of the digital environment on children, which consider the myriad of different activities children undertake in the digital environment, and their evolving capacities and vulnerabilities (OECD, 2022[44]).

The revised OECD Going Digital Measurement Roadmap, which recognises that national statistical systems need to adapt and expand to reflect the digitalisation of economies and societies, can help policy makers build their evidence base and align their countries' priorities for measuring digital transformation using common methodologies and approaches (OECD, 2022[45]).

Soft measures to complement regulation and enforcement

Laws, regulations and enforcement need complementary actions to advance digital safety and protect and empower people online. Business initiatives might include pledges by online marketplaces to mitigate the provision of unsafe products (OECD, 2021[46]) or ethical standards for businesses to promote consumer-friendly user-interface design. These could help businesses improve their reputation and strengthen users' trust. Likewise, voluntary actions by business play an important role in mitigating risks, such as in terms of information security. These include actions and mechanisms to prevent unauthorised access, damage or interference; information security policies; and risk assessment.

Initiatives that take a ‘by-design’ approach offer promising strategies. Some are well-known, such as privacy-by-design and security-by-design, which articulate principles and baseline factors to be considered in the design phase of a service or product and embedded in its operation (OECD, 2020[47]). Digital-safety-by-design is newer but gaining traction as a policy objective and several definitions have emerged in recent years. Some governments and international civil society organisations stress that it implies putting user-safety considerations at the centre of the development of services and products and, rather than implementing remedies reactively, safety-by-design minimises threats by anticipating, detecting and eliminating harms before they occur (eSafety, n.d.[48]).

Technical measures can address risks as well. Examples include tools such as AI-based web crawlers for consumer authorities to detect and mitigate dark patterns or unsafe products online. In 2022, the European Commission launched an e-surveillance tool to help national authorities detect online offers of unsafe products signalled in Safety Gate, the EU alert system for dangerous non-food products (EC, 2022[49]). Other tools allow businesses to self-audit their online choice architecture, and consumers to protect themselves from dark patterns such as browser plugins that automatically communicate consumers’ privacy decisions to the business without needing to respond to a cookie consent notice.

Education and awareness-raising measures point citizens and consumers to information, or help them avoid online harms or make complaints. Guidance can be specific to certain groups, such as consumer campaigns focused on children or consumers with less developed digital skills (OECD, forthcoming[24]). Digital education more broadly is key to protecting and empowering people online. Many OECD countries have a digital education strategy or integrate the topic into a strategy on digital innovation. Digital literacy initiatives are often directed towards children, which is essential, but these should also target broad audiences, for example to enhance consumers’ financial choices (OECD, 2020[50]), upskill or reskill workers, impart digital skills to senior citizens, or support parents, carers and teachers (and local administrations and education authorities) in understanding technologies so as to guide children. It is important that there is equitable access to digital literacy programs, particularly for children. It is observed that social and cultural differences can create mismatch in digital literacy skills, which can exacerbate certain risks. For example, a greater level of digital literacy on the part of a cyberbully can create the power imbalance that is inherent in many forms of bullying.

But while such initiatives and tools play an important role, they are likely insufficient in isolation and should complement robust regulatory and enforcement measures.

Conclusion: Staying ahead of the curve

On one hand, Yoko and Antonio’s family benefit from digital transformation as citizens, consumers and workers. Consumer experiences have improved, social interaction and inclusion amplified, the relationship between citizens and government transformed, and workers’ potential expanded. On the other hand, there are significant risks related to new, online forms of harmful commercial practices; harmful and illegal content; threats to privacy, personal data protection and freedom of expression; and algorithmic discrimination and bias.

The rapid advances and broad uptake of new technologies suggests that the scale and nature of vulnerability in the digital age are changing quickly. Some of us continue to be disproportionately vulnerable – particularly disadvantaged, marginalised, minority and underrepresented groups. But in today’s digital environment, most if not all of us can be vulnerable in different times and contexts. In the consumer space, several scholars have called for a revised understanding of consumer vulnerability as universal or systemic (OECD, forthcoming[24]).

Technological trends such as the increasing ubiquity of AI and the Internet of Things are set to continue. They will be accompanied by emerging trends such as immersive technologies (e.g. augmented and virtual reality). These evolutions will require swift and innovative approaches to guarantee the safety and rights of generations to come.

The CDEP Ministerial meeting is an opportunity for high-level policy makers to consider whether and how measures and concepts need to be adapted, how a human-centric, people-focused digital transformation can be maintained, and how mutual goals can be met. It is in this sense that rights in the digital age find relevance: How are our rights in the offline world applicable to the digital world? Does this new reality drive a need to articulate rights specific to the digital world? In adapting such measures, policies must go the extra mile to empower all members of society, including those more susceptible to harm. The OECD provides research and policy advice on all these matters as a forum for discussion.

Notes

[1] See for example: the 2021 G20 High Level Principles for Children Empowerment and Protection; the 2021 G7 Internet Safety Principles; the 2021 G7 Principles to tackle Online Violence Against Women and Girls and an Action plan to combat Child Sexual Exploitation and Abuse; the 2019 Christchurch Call; and the 2019 G20 Osaka Leaders Statement on Preventing Exploitation of the Internet for Terrorism and Violent Extremism Conducive to Terrorism (VECT).

[2] See, for example, the European Commission's proposed Artificial Intelligence Act.

[3] See for example: Australia (Online Safety Act), Canada (legislative and regulatory proposal to confront harmful content online), the Digital Services Act (European Union), Germany (*Netzwerkdurchsetzungsgesetz* Act to Improve Enforcement of the Law in Social Networks), Ireland (Online Safety and Media Regulation Bill), New Zealand (Films, Video and Publications Classification (Urgent Interim Classification of Publications and Prevention of Online Harm) Amendment Bill), the United Kingdom (Online Safety Bill) or the United States (Platform Accountability and Consumer Transparency Act, 'PACT ACT').

[4] For example, the EU proposal for a directive on combatting violence against women and domestic violence specifically addresses online violence, and Australia's Online Safety Act has specific provisions related to image-based abuse.

References

ACCC (2019), *Digital Platforms Inquiry Final Report*, https://www.accc.gov.au/system/files/Digital%20platforms%20inquiry%20-%20final%20report.pdf (accessed on 24 October 2022). [27]

CoE (2018), *Guidelines to respect, protect and fulfil the rights of the child in the digital environment*, https://rm.coe.int/guidelines-to-respect-protect-and-fulfil-the-rights-of-the-child-in-th/16808d881a (accessed on 24 October 2022). [35]

Conseil d'État (2016), *Fundamental rights in the Digital Age*, https://www.conseil-etat.fr/en/Media/actualites/documents/reprise-_contenus/rapports-et-etudes/fundamental-rights-in-the-digital-age.pdf (accessed on 24 October 2022). [31]

CRC (2021), *General Comment no. 25 on Children's Rights in Relation to the Digital Environment*, https://www.ohchr.org/en/documents/general-comments-and-recommendations/general-comment-no-25-2021-childrens-rights-relation (accessed on 24 October 2022). [36]

Di Geronimo, L. et al. (2020), *UI Dark Patterns and Where to Find Them: A Study on Mobile Applications and User Perception*, Association for Computing Machinery, New York, NY, USA, https://doi.org/10.1145/3313831.3376600. [10]

EC (2022), *Declaration on European Digital Rights and Principles*, https://digital-strategy.ec.europa.eu/en/library/declaration-european-digital-rights-and-principles (accessed on 24 October 2022). [33]

EC (2022), *EU proposes directive to protect the rights of platform workers*, https://ec.europa.eu/eures/public/eu-proposes-directive-protect-rights-platform-workers-2022-03-17_en (accessed on 24 October 2022). [30]

EC (2022), *Proposal for a Regulation of the European Parliament and of the Council laying down rules to prevent and combat child sexual abuse*, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2022%3A209%3AFIN&qid=1652451192472 (accessed on 24 October 2022). [28]

EC (2022), *Safety Gate: Motor vehicles and toys top the list of dangerous non-food products this year*, https://ec.europa.eu/commission/presscorner/detail/en/IP_22_1343 (accessed on 24 October 2022). [49]

eSafety (n.d.), *Safety by Design*, https://www.esafety.gov.au/about-us/safety-by-design (accessed on 24 October 2022). [48]

FNIGC (n.d.), *First Nations principles of ownership, control, access, and possession*, https://fnigc.ca/ocap-training/ (accessed on 24 October 2022). [20]

FTC (2022), *FTC Report Warns About Using Artificial Intelligence to Combat Online Problems*, [16] https://www.ftc.gov/news-events/news/press-releases/2022/06/ftc-report-warns-about-using-artificial-intelligence-combat-online-problems (accessed on 24 October 2022).

FTC (2021), *Age of Learning, Inc. (ABCmouse)*, https://www.ftc.gov/legal-library/browse/cases-proceedings/172-3186-age-learning-inc-abcmouse (accessed on 24 October 2022). [8]

FTC (2021), *FTC Bans SpyFone and CEO from Surveillance Business and Orders Company to Delete All Secretly Stolen Data*, https://www.ftc.gov/news-events/news/press-releases/2021/09/ftc-bans-spyfone-ceo-surveillance-business-orders-company-delete-all-secretly-stolen-data (accessed on 24 October 2022). [17]

Gambling Commission (2019), *Young People and Gambling 2019*, https://www.gamblingcommission.gov.uk/statistics-and-research/publication/young-people-and-gambling-2019 (accessed on 24 October 2022). [12]

Government of Spain (2021), *Charter of Digital Rights*, https://portal.mineco.gob.es/RecursosArticulo/mineco/ministerio/participacion_publica/audiencia/ficheros/Charter%20of%20Digital%20Rights.pdf (accessed on 24 October 2022). [32]

ICO (2021), *The Information Commissioner's position paper on the UK Government's proposal for a trusted digital identity system*, https://ico.org.uk/media/about-the-ico/documents/2619686/ico-digital-identity-position-paper-20210422.pdf (accessed on 24 October 2022). [3]

ICO (2018), *Investigation into the use of data analytics in political campaigns*, https://ico.org.uk/media/action-weve-taken/2260271/investigation-into-the-use-of-data-analytics-in-political-campaigns-final-20181105.pdf (accessed on 24 October 2022). [14]

Ministry of Science and ICT, Republic of Korea (2022), *대한민국 디지털 전략 발표, [Korea Digital Strategy Announcement]*, https://www.msit.go.kr/bbs/view.do?sCode=user&mId=113&mPid=112&pageIndex=3&bbsSeqNo=94&nttSeqNo=3182193&searchOpt=ALL&searchTxt= (accessed on 24 October 2022). [34]

OECD (2022), *Companion Document to the OECD Recommendation on Children in the Digital Environment*, OECD Publishing, Paris, https://doi.org/10.1787/a2ebec7c-en. [44]

OECD (2022), "Dark commercial patterns"*, OECD Digital Economy Papers*, No. 336, OECD Publishing, Paris, https://doi.org/10.1787/44f5e846-en. [9]

OECD (2022), "Enhancing online disclosure effectiveness"*, OECD Digital Economy Papers*, No. 335, OECD Publishing, Paris, https://doi.org/10.1787/6d7ea79c-en. [26]

OECD (2022), *Expert Workshop on Data Ethics: Balancing Ethical and Innovative Uses of Data (internal document)*, OECD, https://one.oecd.org/document/DSTI/CDEP/DGP(2022)1/en/pdf. [19]

OECD (2022), *Measuring Digital Platform Employment and Work (internal document)*, https://one.oecd.org/document/WISE/CSSP(2022)4/en/pdf. [1]

OECD (2022), "Measuring Financial Consumer Detriment in E-Commerce"*, OECD Digital Economy Papers*, No. 326, OECD Publishing, Paris, https://doi.org/10.1787/4055c40e-en. [5]

OECD (2022), *Mis- and dis-information: What governments can do to reinforce democracy (internal document)*, https://one.oecd.org/document/GOV/PGC(2022)8/REV1/en/pdf. [18]

OECD (2022), *Recommendation of the Council on International Regulatory Co-operation to Tackle Global Challenges*, OECD, https://legalinstruments.oecd.org/en/instruments/OECD- [43]

LEGAL-0475.

OECD (2022), *Review of the 2007 OECD Recommendation on Cross-Border Co-operation in the Enforcement of Laws Protecting Privacy (internal document)*, https://one.oecd.org/document/DSTI/CDEP/DGP(2022)2/en/pdf. [40]

OECD (2022), "The OECD Going Digital Measurement Roadmap", *OECD Digital Economy Papers*, No. 328, OECD Publishing, Paris, https://doi.org/10.1787/bd10100f-en. [45]

OECD (2022), *VTRF web portal*, https://www.oecd-vtrf-pilot.org/. [39]

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. [13]

OECD (2021), *Communiqué on product safety pledges*, OECD, https://www.oecd.org/digital/consumer/communique-product-safety-pledges.pdf. [46]

OECD (2021), "Implementation toolkit on legislative actions for consumer protection enforcement co-operation", *OECD Digital Economy Papers*, No. 310, OECD Publishing, Paris, https://doi.org/10.1787/eddcdc57-en. [42]

OECD (2021), *Recommendation of the Council for Agile Regulatory Governance to Harness Innovation*, OECD, https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0464. [41]

OECD (2021), *Recommendation of the Council on Children in the Digital Environment*, OECD, https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0389. [21]

OECD (2020), *OECD Digital Economy Outlook 2020*, OECD Publishing, Paris, https://doi.org/10.1787/bb167041-en. [47]

OECD (2020), "Protecting children online: An overview of recent developments in legal frameworks and policies", *OECD Digital Economy Papers*, No. 295, OECD Publishing, Paris, https://doi.org/10.1787/9e0e49a9-en. [38]

OECD (2020), *Recommendation of the Council on Consumer Product Safety*, OECD, https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0459. [23]

OECD (2020), *Recommendation of the Council on Financial Literacy*, OECD, https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0461. [50]

OECD (2019), *OECD Employment Outlook 2019: The Future of Work*, OECD Publishing, Paris, https://doi.org/10.1787/9ee00155-en. [29]

OECD (2016), "Online Product Safety Sweep Results: Australian Competition and Consumer Commission", *OECD Digital Economy Papers*, No. 262, OECD Publishing, Paris, https://doi.org/10.1787/5jlnb5q64ktd-en. [7]

OECD (2016), *Recommendation of the Council on Consumer Protection in E-Commerce*, OECD, https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0422. [22]

OECD (2012), *Recommendation of the Council on High-Level Principles on Financial Consumer Protection*, OECD, https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0394. [25]

OECD (forthcoming), "Consumer Vulnerability in the Digital Age", *OECD Digital Economy Papers*, OECD Publishing, Paris. [24]

OECD (forthcoming), “OECD Online Product Safety Sweep: Summary Report”, *OECD Digital Economy Papers*, OECD Publishing, Paris. [6]

OECD (n.d.), *The OECD Going Digital Toolkit*, https://goingdigital.oecd.org/. [4]

OHCHR (n.d.), *B-Tech Project OHCHR and business and human rights*, https://www.ohchr.org/en/business-and-human-rights/b-tech-project (accessed on 24 October 2022). [37]

Tribunal of Bologna (2020), *Labour Section, decision of 31 December 2020*, https://www.ansa.it/emiliaromagna/notizie/2021/01/02/rider-cgilalgoritmo-discrimina-sentenza-tribunale-bologna_cc14c299-2c6b-411b-b677-496549ee3af1.html (accessed on 24 October 2022). [2]

WeProtect Global Alliance (2021), *Global Threat Assessment*, https://www.weprotect.org/global-threat-assessment-21/ (accessed on 24 October 2022). [15]

Zendle, D. et al. (2020), *The prevalence of loot boxes in mobile and desktop games*, Addiction, https://doi.org/10.1111/add.14973. [11]