UNITED NATIONS CONFERENCE ON TRADE AND DEVELOPMENT

Artificial Intelligence and Consumer Protection

Technical note produced within the framework of UNCTAD informal Working Group on Consumer Protection in e-commerce

Acknowledgements

This technical note was written by Professor Christine Riefa, Coordinator of the UNCTAD informal Working Group on Consumer Protection in e-commerce (WGE), and Valentina Rivas, Programme Management Officer, Competition and Consumer Policies Branch, UNCTAD, with substantive inputs from UNCTAD secretariat, Elizabeth Gachuiri and Arnau Izaguerri from the Division of International Trade and Commodities (DITC), and Torbjorn Fredriksson, Pilar Fajarnes Garces, Antonio Vezzani and Wai Kit, Si Tou from the Division on Technology and Logistics (DTL) under the general coordination of Teresa Moreira, Head of the Competition and Consumer Policies Branch (DITC). In addition, UNCTAD received contributions from the Department of Consumer Affairs, Government of India; Italian Competition Authority (AGCM); Office of the Federal Prosecutor for the Consumer (PROFECO), Mexico; and the Office of Competition and Consumer Protection (UOKiK), Poland.

Note

This note was developed within the framework of UNCTAD informal working group on consumer protection in e- commerce, as mandated by the Intergovernmental group of experts on consumer protection law and policy in its eighth session of 1 and 2 July 2024. The UNCTAD informal working group on consumer protection in e-commerce, established following a request by the Intergovernmental Group of Experts at its second session in 2017, serves as a platform to promote the exchange of information, highlight best practices, and advance discussions on consumer protection in e-commerce, under the leadership of member States on a voluntary basis and without financial implications for the United Nations regular budget. The group meets regularly through informal virtual meetings and is open to government representatives with relevant expertise—such as national consumer protection authorities—as well as interested international organizations, networks, civil society, and academia. Its mandate has been renewed annually by the Intergovernmental Group of Experts, to which it reports on its activities and outcomes. Since 2023, the informal working group has been examining the implications of Artificial Intelligence for consumer protection. Three webinars have been held to discuss the risks consumers may face,[1] the potential benefits for both consumers and consumer protection agencies,[2] and practical examples of AI tools already deployed by agencies to support their work, enhance efficiency, and strengthen enforcement.[3]

[1] See: https://unctad.org/meeting/webinar-artificial-intelligence-and-consumer-protection-risks-consumers

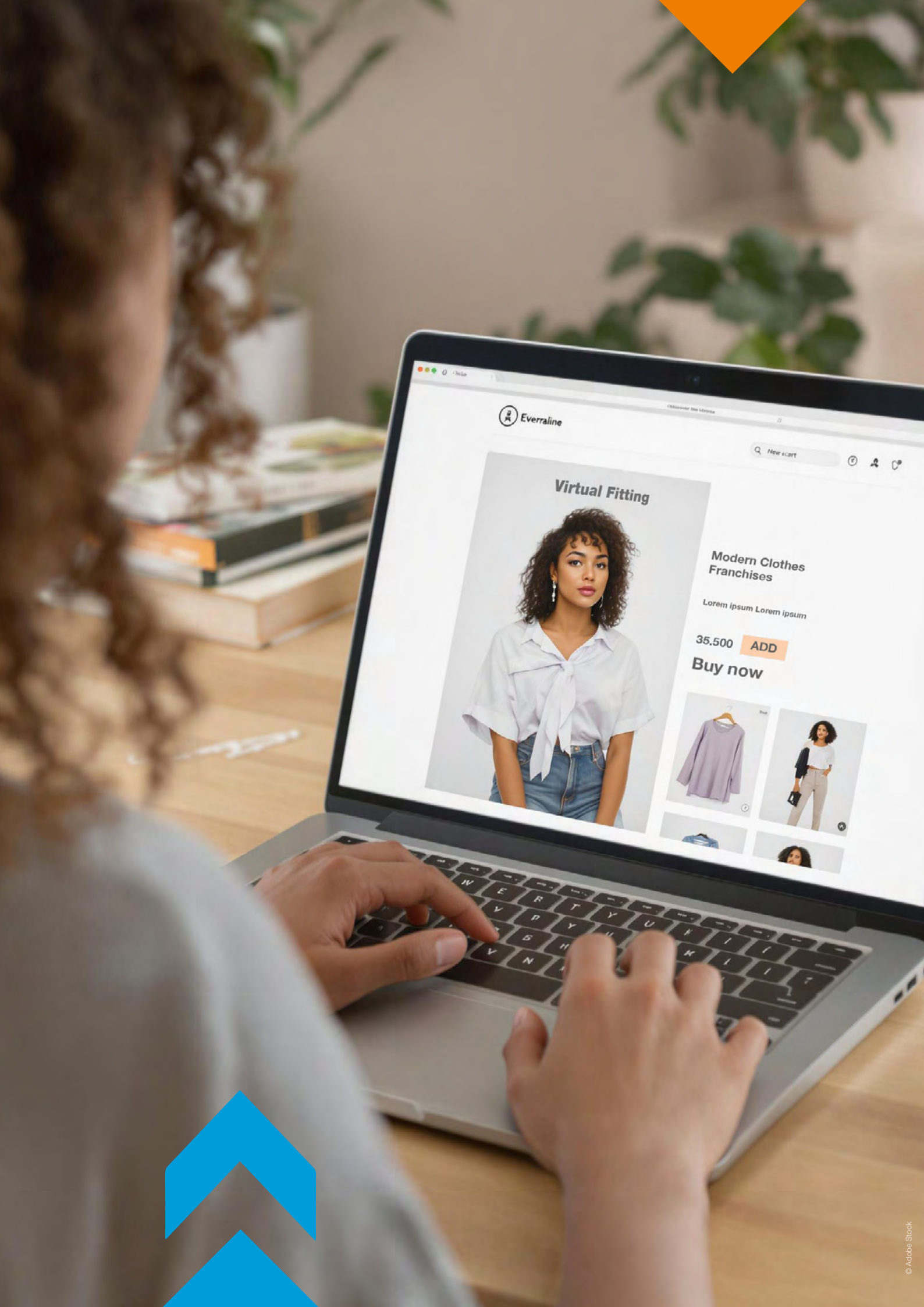
[2] See: https://unctad.org/meeting/webinar-artificial-intelligence-and-consumer-protection-harnessing-tech-better-enforce

[3] See: https://unctad.org/meeting/webinar-artificial-intelligence-deployment-consumer-protection-enforcement-authorities

Table of contents

Chapter 1

Introduction


Everraline
Virtual Fitting
Modern Clothes
Franchises
Lorem ipsum Lorem ipsum
35.500
ADD
Buy now

The accelerating integration of artificial intelligence (AI) into global digital markets is ushering in a new era of commerce and consumption. As AI reshapes how consumers interact in markets—whether through recommendation engines, automated dispute resolution, or virtual shopping assistants—its impact is being felt in both transformative opportunities and complex risks. This duality is at the heart of the current discourse, where consumer protection agencies around the world are grappling with how to ensure that AI empowers rather than endangers consumers. This note by UN Trade and Development (UNCTAD) provides a timely and comprehensive exploration of the intersection between AI and consumer protection, charting both the benefits and pitfalls of AI in electronic commerce, and mapping the proactive initiatives undertaken by enforcement agencies to adapt to a rapidly evolving technological landscape.

At its most promising, AI presents unprecedented opportunities to enhance consumer welfare. It can facilitate better decision-making through personalized content, assist in identifying unfair practices such as dark commercial patterns or misleading advertisements, and streamline dispute resolution via advanced online platforms. Enforcement authorities are beginning to harness these innovations to detect harmful practices in real-time, transform reactive enforcement into preventive action, and improve transparency and accountability in digital markets. However, the same capabilities that make AI valuable also present significant risks. The technology can be—and increasingly is—used to mislead, manipulate, and defraud consumers through opaque algorithms, invasive data collection, and the proliferation of deepfakes and synthetic content. Furthermore, AI's heavy reliance on vast quantities of data exacerbates privacy concerns, heightens the risk of discrimination, and compounds the challenges of ensuring environmental sustainability.

This technical note, developed under the auspices of UNCTAD's informal working group on consumer protection in e-commerce, unpacks this complex reality. It brings together global experiences, regulatory responses, and technological strategies deployed by consumer protection agencies, particularly in light of the growing influence of generative AI and existing models in business-to-consumer transactions. The scope of the analysis spans not only the technological applications in commercial settings for consumers but also the institutional transformations that are needed and that are taking place within enforcement bodies to meet the challenges AI poses.

At the global level, momentum is building for human-centric, rights-based, and inclusive AI governance. Initiatives such as the UNESCO Recommendation on the Ethics of AI[4] (2021), the "AI for Good Global Summit" — a United Nations platform led by the International Telecommunication Union (ITU) that promotes the use of AI for sustainable development[5] — and the Secretary-General's High-Level Advisory Body on AI reflect growing international consensus on ethical AI deployment.[6] Importantly, it recognized the necessity of addressing unchecked power and ensuring consumer rights and fair competition.[7] Despite the advances in the discussions, regulatory responses remain uneven, particularly in developing countries,

> AI in e-commerce offers transformative benefits for consumers and enforcement agencies but brings significant risks such as manipulation, opacity, and privacy violations that demand urgent attention from consumer protection stakeholders.

[4] https://www.unesco.org/en/articles/unesco-adopts-first-global-standard-ethics-artificial-intelligence

[5] The AI for Good Global Summit, organized annually since 2017 by the International Telecommunication Union (ITU) and 40 United Nations agencies, is a leading platform promoting AI for advancing global development priorities like health, climate, gender, and sustainable infrastructure. In 2023, the summit introduced *AI Governance Day*, which highlighted the "AI governance paradox". The paradox outlines that while regulation is often seen as lagging technological advancements, the lack of adequate tools to monitor and control AI systems poses significant risks.

[6] UN chief says regulation needed for AI to 'benefit everyone' | UN News

[7] AI Advisory Body, Governing Ai for Humanity, final report (September 2024) p. 36. See: https://www.un.org/sites/un2.un.org/files/governing_ai_for_humanity_final_report_en.pdf

underscoring the importance of peer learning, technical assistance, and stronger cooperation to bridge capability gaps.

Chapters 2 through 45 delve into the applications of AI in e-commerce and the multifaceted risks they entail. AI is redefining digital consumption, optimizing practically everything from product visibility to pricing strategies, and often doing so without the consumer's knowledge or consent. Further, it also enables covert manipulation that blurs the line between persuasion and coercion. The risks extend further into algorithmic discrimination, opaque decision-making, and environmental degradation due to the resource-intensive nature of AI systems. In response, the note calls for the establishment of clear regulatory frameworks that explicitly incorporate consumer protection considerations—bridging the gap between broad AI governance and the specific vulnerabilities of consumers.

The note also explores avenues to address AI challenges that go over regulation. Chapters 5 to 7 highlight how consumer protection enforcement agencies themselves are evolving, harnessing AI and other digital tools to better serve and protect consumers. From Poland's ARBUZ system, which identifies unfair contract terms using natural language processing, to Brazil's high-volume online dispute resolution platform, agencies are embracing AI to increase efficiency, improve targeting, and hamper harmful practices. These examples demonstrate how technology can support not only the detection and sanctioning of violations but also consumer empowerment and education.

Yet, these advances are not without challenge, especially for developing countries. The note underscores that effective AI deployment depends on access to high-quality, representative, and structured data—resources that many agencies currently lack. Furthermore, the deployment of AI must be guided by ethical principles to prevent the perpetuation of bias and discrimination. To this end, consumer protection agencies are encouraged to invest in technological infrastructure, build in-house expertise, and adopt data governance practices that enhance the reliability and fairness of AI tools.

Finally, the note turns to international cooperation as an indispensable pillar for equitable AI deployment. With AI adoption advancing at different speeds and depths across regions, collaborative frameworks, knowledge sharing, and resource pooling are vital. It shows global initiatives emphasizing the need for capacity building to ensure equitable AI enforcement. UNCTAD's central role in fostering such cooperation is highlighted, alongside the need for tailored support to developing countries to close the digital and regulatory divide.

This note serves as a key input to the 9th United Nations Conference to Review All Aspects of the Set of Multilaterally Agreed Equitable Principles and Rules for the Control of Restrictive Business Practices, scheduled to take place under the auspices of UNCTAD in July 2025. It serves as both a cautionary tale and a roadmap. It makes clear that while AI has the potential to improve consumer outcomes, it also intensifies existing risks and introduces new ones that traditional enforcement methods may not adequately address. The way forward lies in a holistic approach that combines regulation, innovation, education, and collaboration. For policymakers and enforcement agencies alike, the challenge is not whether to engage with AI, but how to do so in a manner that is transparent, inclusive, and just. Through this lens, the note sets a compelling agenda for ensuring that AI becomes a tool for consumer empowerment—not exploitation—and a force for a fairer and more resilient digital economy.

Chapter 2

Use of Artificial Intelligence in electronic commerce

Understanding the origins and scope of AI is key to grasping its impact on consumers. The Dartmouth Summer Research Project on Artificial Intelligence, held in 1956, is frequently considered the genesis of AI as an established field of academic study, building upon earlier theoretical foundations. Artificial Intelligence is a wide-ranging concept, for which there is no globally agreed definition. According to Coll and Riefa (2024), AI can be described as 'a collection of advanced software technologies and applications that allow machines to simulate different aspects of human intelligence, most critically learning and decision making'.[8] These characteristics make AI applicable in many environments where human discernment is required.

The type of AI that attracts most attention and scrutiny is generative AI, which refers to the use of AI technology to create new content (such as music, text, images, audio, or videos). Generative AI is powered by foundation models, which are large-scale AI systems trained on extensive datasets capable of supporting a wide range of applications.[9] These models rely on machine learning, a branch of AI that enables systems to improve their performance through data-driven learning rather than following pre-programmed instructions for specific tasks. While the terms AI and machine learning are often used interchangeably, they are not the same.[10] Machine learning[11] refers specifically to the techniques that allow systems to learn and improve from data. The most recent models on the market are already showing the potential to transform sectors like e-commerce, opening new possibilities for businesses and consumers alike.

AI is transforming e-commerce while also enabling sophisticated forms of consumer manipulation. AI-enabled tools have become increasingly common in businesses engaged in electronic commerce, transforming how they operate and interact with consumers. According to a recent study,[12] 84 per cent of companies are already using AI to create and manage trade promotions, illustrating the growing role of AI in optimizing commercial strategies. AI is shaping the consumer experience online and offline. Businesses are leveraging AI to improve the accuracy of targeted advertising to consumers,[13] ensuring that marketing messages reach the right audience at the right time. AI is also powering personalized shopping experiences, through tools such as recommender systems and virtual shopping assistants that tailor product suggestions based on consumer preferences. Additionally, AI-driven chatbots are increasingly used to communicate with consumers and offer individual advice.

While useful, those AI applications are also creating a fertile ground for exploiting by deploying practices that are covert and thus cannot easily be detected. Many consumers, for example, are unaware that they are being manipulated by 'dark

AI is revolutionizing e-commerce by personalizing services and optimizing operations, yet it also enables covert manipulation tactics like dark patterns that undermine informed consumer choice and trust.

8 Riefa, Coll, The Transformative potential of Enforcement Technology (EnfTech) in Consumer Law (2024), https://www.enftech.org/report Annex 1 Technologies and data: terms in use, p.76. Note, the OECD defines AI systems as: *'a machine-based system that for explicit or implicit objectives, infers, from the input it receives, how to generates outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments. Different AI systems vary in their levels of autonomy and adaptiveness after deployment.'* https://oecd.ai/en/wonk/ai-system-definition-update.

9 CMA, AI Foundation Models: Initial Report (2022), p.9 https://www.gov.uk/government/news/proposed-principles-to-guide-competitive-ai-markets-and-protect-consumers.

10 Riefa, Coll, The Transformative potential of Enforcement Technology (EnfTech) in Consumer Law (2024), Annex 1 Technologies and data: terms in use, p.76.

11 There are many types of machine learning, including supervised/ un-supervised, reinforcement, deep learning, neural networks, natural language processing, all performing tasks using different methods.

12 Embedding AI in your brand's DNA, IBM (2025): https://www.ibm.com/downloads/documents/us-en/115d460037d51479

13 Agnieszka Jabłonowska and others, 'Consumer Law and Artificial Intelligence Challenges to the EU Consumer Law and Policy Stemming from the Business' Use of Artificial Intelligence' 89, p.23.

patterns'[14] a growing concern reported by all agencies participating in a recent UNCTAD survey.[15] These deceptive techniques take various forms. *Default settings* may silently enable tracking or data collection without the user's knowledge. *Confirmshaming* pressures users into accepting offers by wording opt-out choices in a way that induces guilt or embarrassment—such as displaying messages like *"No thanks, I don't care about saving money"*. *Urgency and scarcity cues* falsely suggest that a product is almost sold out or that an offer is expiring soon, prompting rushed decisions. *"Roach motel" tactics* make it easy to sign up for subscriptions or services but intentionally difficult to cancel them later. Other common practices include *hiding extra fees* until the final stage of checkout, *sneaking items* into shopping carts without clear consent, or *pre-ticking consent boxes* for unwanted services or data collection. These techniques are increasingly automated or amplified by AI systems, making it even harder for consumers to recognize manipulation or protect themselves.

[14] There is no agreed definition of the term "dark commercial patterns". According to one definition by OECD, the term "dark commercial patterns" refers to a wide variety of practices commonly found in online user interfaces that lead consumers to make choices that may not be in their best interests, including by exploiting consumer biases. They typically seek to get consumers to give up more money, personal data or attention time than desired. In this way, they are inextricably linked to an underlying business model, even if user interface designers may often bear no malicious intent.

[15] Within the UN Trade and Development informal working group on consumer protection in e-commerce, led by Argentina and Kenya in 2021, member States shared experiences with various dark commercial patterns. These include, for example, default settings that covertly track and monitor user activity; "confirm shaming" which manipulates consumers into making certain choices; artificially created urgency and scarcity mechanisms that accelerate purchasing decisions; "roaching," which traps consumers in difficult-to-escape situations; and "hidden costs" and last-minute product additions at the time of purchase. In response to these business practices, some countries (e.g. Argentina and Germany) have implemented a compulsory "cancellation button" that must remain accessible to consumers. The working group also advocated for strengthened collaboration among consumer protection agencies and improving business guidance with self-assessment tools.

Chapter 3

Key concerns: digital divide, data protection, competition, and environment

The use of AI is growing rapidly, yet significant digital gaps persist across regions. Estimations reveal that the world is inching towards universal access, with 96 per cent of the global population, in 2024, covered by a mobile broadband network enabling Internet access, and therefore access to AI.[16] However, significant gaps remain. For instance, in rural areas of low-income countries, nearly 30 per cent of the population lacks the possibility of connecting to the Internet. For the world's most vulnerable communities, digital exclusion exacerbates existing challenges. These gaps not only limit access to the benefits of AI but also highlight the need to intensify efforts to remove barriers that keep people offline and close the usage gap.

AI and its ability to orient a consumer journey from the outset to the act of consumption, including product selection, pricing, payment systems and delivery methods, also poses some risks. Those include the potential to impact on free choice, causing not only detriment to consumers but also further disrupting competition.

AI can be used to manipulate consumer choice. 'AI washing'[17] refers to the practice of companies overstating their AI capabilities, creating a deceptive facade of innovation claims that are increasingly being detected by enforcement authorities. In India for example, there has been a proliferation of products and services claiming to use AI as a selling point where the underlying technology is in fact not based on artificial intelligence.[18] In addition, AI-powered recommender systems and targeted advertising are being used to shape consumer decisions by pushing personalized content or product suggestions based on user data, often without consumers realizing how their preferences are being influenced. Some dangers reside in the fact that end users may be conditioned to trust the output of AI generated content such as product recommendations, regardless of their accuracy or reliability, partly because of AI's ability to mimic human language. The marketing strategies used by the creators of AI models can further contribute to consumer harm when description of AI capabilities are deliberately vague or misleading fostering misplaced trust in these systems.[19]

AI can also be used to further enhance surveillance advertising strategies, where targeting is based not simply on browsing preferences but on real time exchanges with consumers and the collection of humans generated conversational data. In this sphere, the excesses of some AI chatbot[20], or the services based on the formation of romantic relationships are a case in point.[21] The same technology can also be used to nudge or worse, manipulate[22] consumers into buying decisions.

> The risks of AI to consumers include invasive data collection, algorithmic discrimination, market distortion, fraud, and environmental harm, all exacerbated by governance gaps and the dominance of powerful private actors.

[16] ITU Measuring digital development: Facts and Figures 2024: https://www.itu.int/en/ITU-D/Statistics/pages/facts/default.aspx

[17] AI washing refers to the making of claim that products are AI powered where they are not or overstating the AI capabilities of products, creating a deceptive facade of innovation. The term "AI washing" is like the concept of "greenwashing," where companies exaggerate their environmental efforts.

[18] Video to the webinar on artificial intelligence and consumer protection: Risks for consumers, and presentation slides from the Department of Consumer Affairs Government of India.

[19] Norwegian Consumer Council, Ghost in the machine (June 2023) para 2.2.2., p. 24.

[20] https://www.theguardian.com/technology/2023/feb/17/i-want-to-destroy-whatever-i-want-bings-ai-chatbot-unsettles-us-reporter

[21] In 2023, the Italian Data Protection Authority found that Replika (a Generative AI powered application that simulates a partner) was collecting personal data from children without a legal basis and was in breach of the GDPR leading to changes in the way the service operates. The Competition and Markets Authority in Italy has also acted on misleading and aggressive practices notably in the online gaming sector notably for the use of loot boxes (PS11594 ELECTRONIC ARTS-Acquisti nei videogiochi e PS11595 - ACTIVISION BLIZZARD-Acquisti nei videogiochi.) as well as against social media (tik-tok) for failing to implement adequate content supervision mechanisms, particularly concerning videos depicting self-harm.

[22] https://www.forbes.com/sites/elijahclark/2023/11/28/how-retailers-are-using-ai-to-manipulate-consumer-shopping/ see also https://www.fastcompany.com/90871955/how-generative-ai-is-changing-surveillance-capitalism.

AI can be harnessed not simply to mislead but also to defraud consumers. Generative AI can easily be used to make scams less detectable[23], although most generative AI providers clearly state that the technology should not be used for fraudulent purposes.[24] For instance, scammers have started using large language models to generate convincing phishing messages that are free of the spelling and grammar mistakes that typically helped consumers identify fraud in the past[25] In one documented case, a reporter successfully used AI-generated audio deepfakes to bypass the voice recognition security system on his own bank account, illustrating how voice cloning can undermine biometric security systems and enable fraud.[26] Deepfakes can also be used to with alarming effectiveness in consumer fraud[27] and AI generating text can be equally skilled in spreading misleading information and influencing consumer choice.

This is particularly concerning because humans remain relatively unreliable at identifying AI-generated content, often failing to recognize when they are interacting with a machine rather than a real person..[28] AI itself is also notoriously poor at detecting other AI generated content.[29] Studies[30] have also shown that human users are more likely to trust AI generated text and thus can be more easily deceived at scale. This can create a perfect storm for consumers unable to detect or avoid unfair commercial practices online. Consumers are also prone to economic and emotional harm in the absence of any direct lines of redress or inability to influence market corrections. Moreover, generative AI can be exploited to further refine or automate sophisticated cybercrime operations.[31]

Consumer privacy is under threat. Currently AI models can be trained using vast amount of personal information that consumers have shared online, such as social media posts, reviews or browsing history, often without the explicit knowledge or informed consent. Beyond using this existing data, AI systems are capable of inferring or generating additional personal data through techniques like profiling, predictive analytics or data aggregation.[32] For example, AI can analyze a person's online behavior and infer sensitive attributes, such as political opinions, health status,

[23] See for a comprehensive account, Europol Tech Watch Flash, Chat GPT, the impact of large language models on law enforcement (2023) p. 7-9, https://www.europol.europa.eu/publications-events/publications/chatgpt-impact-of-large-language-models-law-enforcement

[24] Tali Ramsey, Are AI chatbots risking a new wave of convincing scams? (Which?, 27 October 2023).

[25] Tali Ramsey, Are AI chatbots risking a new wave of convincing scams? (Which?, 27 October 2023); Europol, Facing Reality? Law enforcement and the challenge of deepfakes, an observatory report form the Europol Innovation Law (2022) https://www.europol.europa.eu/publications-events/publications/facing-reality-law-enforcement-and-challenge-of-deepfakes

[26] Norwegian Consumer Council, Ghost in the machine (June 2023) p. 32 citing Jakesch, Hancok and Naaman, Human heuristics for AI generated language are flawed (2023) https://doi.org/10.1073/pnas.2208839120

[27] Europol, Facing Reality? Law enforcement and the challenge of deepfakes, an observatory report form the Europol Innovation Law (2022) https://www.europol.europa.eu/publications-events/publications/facing-reality-law-enforcement-and-challenge-of-deepfakes

[28] Norwegian Consumer Council, Ghost in the machine (June 2023) p. 25 citing Jakesch, Hancok and Naaman, Human heuristics for AI generated language are flawed (2023) See: https://doi.org/10.1073/pnas.2208839120

[29] Norwegian Consumer Council, Ghost in the machine (June 2023) p. 27 citing https://theconversation.com/we-pitted-chatgpt-against-tools-for-detecting-ai-written-text-and-the-results-are-troubling-199774 and https://techcrunch.com/2023/01/31/openai-releases-tool-to-detect-ai-generated-text-including-from-chatgpt/?guccounter=1

[30] Do_You_Trust_ChatGPT? Perceived_Credibility_of_Human_and_AI-Generated_Content: https://www.researchgate.net/publication/373714847_
Zhang Y, Gosline R. Human favoritism, not AI aversion: People's perceptions (and bias) toward generative AI, human experts, and human–GAI collaboration in persuasive content generation. *Judgment and Decision Making*. 2023;18:e41. doi:10.1017/jdm.2023.37

[31] Europol Tech Watch Flash, Chat GPT, the impact of large language models on law enforcement (2023) p. 9.

[32] This can include deepfakes, but also AI hallucinations for example. A similar issue pertains the use of copyrighted materials to train AI models without the permission of the IP owner.

or financial vulnerability, which the person may have never explicitly shared. These AI-generated profiles may not accurately reflect the consumer but can still be used to target them with specific offers, deny them services, or influence their choices. This practice risks producing biased or misleading profiles that can lead to discrimination or unfair treatment. Moreover, such activities often violate data protection and privacy laws, which typically require transparency, fairness, and informed consent when personal data is processed.

Opacity and discrimination are chief concerns. It is not always possible for developers of AI systems to explain how a decision by the system was made.[33] This is because AI learns on its own rather than follow a pre-defined path. The data quality fed into the algorithm ultimately influences the output quality. Hence, AI systems can be prone to abuse, as they often replicate existing inequalities and biases present in the data on which they are trained.[34] In that sense, AI systems can perpetuate existing biases or create new ones, resulting in discrimination against certain groups. For example, AI-powered recruitment tools have been shown to disadvantage women by downgrading their applications,[35] and AI systems used in financial services have been found to reinforce gender bias in credit approvals.[36] This should warrant 'great caution' about the use of AI[37] because it can be inaccurate, biased, discriminatory[38] and lead to a commercial surveillance creep.[39] . The opacity of decision making also makes it more challenging to apportion liability and verify claims made about the efficacy of AI applications, especially when the AI model is not the result of a single entity's work but relies on third party generative AI models. As a result, the risk for consumer harm is acute and finding the entity liable for the harm suffered may be almost (if not) impossible, leaving consumers to shoulder the damage caused by erroneous advice.

To complement regulatory and enforcement efforts, educating consumers about the risks posed by AI-driven manipulation is essential Empowerment initiatives should include public awareness campaigns, interactive tools, and user-friendly guides that demystify AI's role in consumer interactions.

These resources can help consumers identify manipulation tactics, avoid unfair practices, and make autonomous, informed decisions.

The use of AI heightens environmental concerns in e-commerce. While there is evidence that technology can be used to solve aspects of climate change[40], the increased use of AI in an already carbon intensive industry sector is increasing the environmental burden. The UNCTAD

[33] Riefa, Coll, The Transformative potential of Enforcement Technology (EnfTech) in Consumer Law (2024), p.69. The Black box problem is well documented. For a useful overview, see A. Azzutti, W.-G. Ringe and H. S. Stiehl, Machine Learning, Market Manipulation and Collusions on Capital Markets: Why the "Black Box" Matters (2021).

[34] Riefa, Coll, The Transformative potential of Enforcement Technology (EnfTech) in Consumer Law (2024), p.69. The Black box problem is well documented. For a useful overview, see A. Azzutti, W.-G. Ringe and H. S. Stiehl, Machine Learning, Market Manipulation and Collusions on Capital Markets: Why the "Black Box" Matters (2021).

[35] See: Amazon's Sexiest Hiring Algorithm Could Still Be Better Than a Human (November 2018). See: https://imd.widen.net/view/pdf/z7itobahi6/tc061-18-print.pdf

[36] See: Algorithmic Bias, Financial Inclusion, and Gender (February 2021). See: https://www.womensworldbanking.org/wp-content/uploads/2021/02/2021_Algorithmic_Bias_Report.pdf

[37] FTC, Combatting online harms through innovation, A report to Congress (2022) See: https://www.ftc.gov/reports/combatting-online-harms-through-innovation

[38] See: https://unctad.org/system/files/non-official-document/ccpb_WGE_Webinar__A1_Salsburg_en.pdf

[39] FTC report warns about using artificial intelligence to combat online problems (16 June 2022) See: https://www.ftc.gov/news-events/news/press-releases/2022/06/ftc-report-warns-about-using-artificial-intelligence-combat-online-problems

[40] Mateson, 9 ways AI is helping tackle climate change (World Economic Forum, 12 Feb 2024) See: https://www.weforum.org/agenda/2024/02/ai-combat-climate-change/#:~:text=The%20use%20of%20artificial%20intelligence,the%20World%20Economic%20Forum%20says

Digital Economy Report 2024[41] (DER 2024) confirms that the digital economy is resource intensive. For example, a two-kilogram computer uses over 800 kilograms of raw materials while a smartphone requires 70 different materials of which 45 are metals.[42] AI uses more energy than other forms of computing and it is predicted that the integration of large language models into search engines alone could involve a fourfold increase in energy use per individual search query.[43] The DER 2024 notes that recent data from Google and Meta shows that the training phase of a large machine learning model accounts from 20-40 per cent of the overall machine learning related energy use, while 60-70 is used during the application/ use of the model and up to 10 per cent for the model development.[44] There is a risk that in order to continue and expand the use of AI for commercial gains, companies could make 'greenwashing' claims that cannot be verified either because data is not yet available or because, for example, carbon offsetting plans may be used absent a unified methodology for calculation, leading to confusion and ineffective controls.[45] Risks of greenwashing the use of AI in e-commerce is a concern because there is evidence that the practice is common for all types of products and services. In 2022, an UNCTAD report[46] showed that 68 per cent of consumer protection agencies surveyed had received complaints related to misleading or false environmental claims about products in the last five years.

AI is reinforcing existing market power and enabling new forms of anti-competitive behaviour. One of the key risks is structural, with the benefits of AI being currently the purview of only a few private sector actors and an even smaller number of states.[47] The architecture that supports the deployment of AI is based on existing private power structures. There is a growing risk of seeing proprietary AI models embed existing inequalities, giving large technology conglomerates the ability to exclude rivals and further entrench existing dominant positions.[48] This risk is compounded by the fact that technology can facilitate new forms of collusion, such as real time monitoring prices that expand anti-competitive behaviour beyond traditionally concentrated or oligopolistic markets..[49] Besides, AI facilitates the ability to roll out services that were once stand-alone, meaning that consumers can fulfil all needs in a single platform ecosystem, further reinforcing established market structures.[50]

[41] Digital Economy Report 2024: Shaping an environmentally sustainable and inclusive digital future https://unctad.org/system/files/official-document/der2024_en.pdf

[42] Justice et Paix (2019). Les fausses promesses du numérique: Environnement, éducation, santé, travail. Etude. Commission Justice et Paix francophone de Belgique. Brussels. See: C:/Users/valentina.rivas/Downloads/Justice-Paix-Etude-Les-fausses-promesses-du-numerique-05.pdf

[43] Norwegian Consumer Council, Ghost in the machine (June 2023) para 2.7., p. 35.

[44] Digital Economy Report 2024: Shaping an environmentally sustainable and inclusive digital future. See: https://unctad.org/system/files/official-document/der2024_en.pdf

[45] Norwegian Consumer Council, Ghost in the machine (June 2023) para 2.7.3., p. 37.

[46] Superintendence of Industry and Commerce of Colombia - Sub-Working Group on Misleading and Unfair Business Practices (2022). Report on Environmental Claims in E-commerce. See: https://unctad.org/system/files/information-document/ccpb_WG_EC_Report_Environmental_Claims_FINAL_en.pdf

[47] AI Advisory Body, Governing Ai for Humanity, interim report (December 2023) para 12, p.5. https://www.un.org/sites/un2.un.org/files/ai_advisory_body_interim_report.pdf

[48] Norwegian Consumer Council, Ghost in the machine (June 2023) para 2.1.3., p.17 https://storage02.forbrukerradet.no/media/2023/06/generative-ai-rapport-2023.pdf; see also, CMA, AI foundation models update paper (April 2024)

[49] OECD, Algorithms and Collusion – Note from Italy, DAF/COMP/WD(2017)18, p.3, https://one.oecd.org/document/DAF/COMP/WD(2017)18/en/pdf

[50] Norwegian Consumer Council, Ghost in the machine (June 2023) para 2.1.3., p.19.

Chapter 4

Strengthen consumer protection through AI regulation

The absence of clear regulations on AI can risks undermining its safe and responsible adoption. While AI presents enormous potential for innovation, the possibility of misuse—particularly in electronic commerce—is high. According to the UN AI Advisory Body, 'this technology cries out for governance, not merely to address the challenges and risks but to ensure we harness its potential in ways that leave no one behind'.[51] It is also essential to put in place some control so that the use of AI does not become an arms race between different AI players and with enforcement agencies.[52]

Tools and reforms for effective enforcement. As highlighted in the United Nations Guidelines for Consumer Protection (UNGCP), consumer protection policies must be adapted to digital environments.[53] New laws or regulatory guidance may be required to give agencies the tools to enforce fair practices and manage AI risks. This includes both procedural and substantive reforms. On the procedural side, agencies may need powers to investigate and sanction AI-related harm, such as ordering changes to or the removal of harmful AI systems. Substantive rules may address algorithmic manipulation, set red lines for high-risk uses, and ensure remedies are available for consumers harmed by AI-driven practices. Existing frameworks on data protection, unfair commercial practices, and product safety can support this effort, but many countries—especially Least Developed Countries—face capacity constraints that limit their enforcement capabilities.

International efforts and instruments. Complementing national and regional approaches, several international instruments have emerged to guide the ethical and inclusive development of AI. The UNESCO Recommendation on the Ethics of Artificial Intelligence (2021)[54] offers a global framework grounded in human rights, transparency, and accountability. The United Nations General Assembly adopted two resolutions in 2024 — one in March on the promotion of "safe, secure and trustworthy" AI[55] and another in June on AI for sustainable development[56] — both of which stress the importance of capacity building, the protection of human rights, international cooperation and inclusion of developing countries.

Additionally, the 2024 Summit of the Future adopted the Pact for the Future,[57] which includes a Global Digital Compact outlining principles for digital governance.[58] These include the development and use of AI in a rights-based, human-centred, and sustainable manner. These instruments are highly relevant to consumer protection, reinforcing the need for AI to serve the public interest and promote fairness in digital markets.

Current regulatory landscape: national and regional trends. Despite governments beginning to design and implement regulations governing AI, an ITU survey shows that 85 per cent of its 193 member States do not have any AI regulation or policy in place.[59] The same survey indicates that by the end of May 2024, countries like Brazil, China, Estonia, France, India,

Robust regulatory frameworks are essential to ensure AI is used responsibly in e-commerce, requiring new laws and guidance that empower agencies, protect consumers, and align national efforts with international best practices

[51] AI Advisory Body, Governing Ai for Humanity, interim report (December 2023) para 4, p.3. https://www.un.org/sites/un2.un.org/files/ai_advisory_body_interim_report.pdf.

[52] Riefa, Coll, Use of AI Enforcement Technology, in Di Matteo, Poncibo, Howells (eds.), Cambridge Handbook of AI and Consumer Law (Cambridge University Press, forthcoming 2024) 212.

[53] UNGCP 63

[54] https://www.unesco.org/en/articles/unesco-adopts-first-global-standard-ethics-artificial-intelligence

[55] A/78/L.49

[56] A/78/L.86

[57] United Nations Pact for the Future, Global Digital Compact and Declaration on Future Generations (September 2024). See: https://www.un.org/sites/un2.un.org/files/sotf-pact_for_the_future_adopted.pdf

[58] United Nations Pact for the Future, Global Digital Compact and Declaration on Future Generations (September 2024) p. 40. See: https://www.un.org/sites/un2.un.org/files/sotf-the-pact-for-the-future.pdf

[59] AI Governance Day - From Principles to Implementation

Japan, Kazakhstan, Kenya, Republic of Korea, Rwanda, Singapore, United Arab Emirates, United Kingdom, United States of America, and Uruguay have AI governance initiatives in place. Moreover, there are several regional initiatives including the African Union, ASEAN, European Union, and MERCOSUR.[60] These national and regional broader initiatives address various aspects of AI such as safety, data protection, and intellectual property. However, they do not necessarily include provisions specifically aimed at consumer protection, showing an opportunity to build upon existing frameworks to create comprehensive and inclusive regulations that ensure the benefits of AI are shared widely and responsibly in ways that safeguard consumers.

The specific role of consumer protection agencies. Even where new laws are introduced to address AI-related risks, much of the responsibility for consumer protection will likely fall on consumer protection agencies. Some oversights of AI practices can be carried out under existing laws, such as those on data protection, [61] unfair commercial practices, and product safety. [62] However, countries are not starting from the same position, and many—especially Least Developed Countries—may face greater challenges in using existing tools effectively. Stronger regulatory guidance may also be necessary to give agencies the right tools to enforce fair behaviours and control the excesses of AI. This may require procedural as well as substantive regulations. Procedural laws may be necessary if enforcement authorities lack the ability to conduct investigations and order remedies such as modification of an AI tool or its destruction[63] to avoid further harm, or order fines for wrongdoing. Substantive laws may regulate the use of AI and assist in the development of trustworthy AI, banning or tightly controlling practices that present an unacceptable level of risk[64] or provide mechanisms for redress for consumers harmed by AI activity.[65]

National examples of emerging practices. In the United States of America, an executive order on the safe, secure, and trustworthy development and use of AI[66] commits federal agencies to enforcing existing consumer protection laws and principles and enact appropriate safeguards and supports responsible of AI that protect consumers, raise the quality of goods and services, lower their prices, or expand selection and availability.[67] Congress instructed the Federal Trade Commission (FTC) to recommend laws that could advance the use of AI to address online harms leading

[60] AI Governance Day - From Principles to Implementation. Pag 17, 18.

[61] See for example, the intervention of the Italian Data Protection Agency on ChatGPT imposing a temporary limitation on Open AI (the owners of Chat GPT) to address issues with the processing of personal data of Italian citizens, which did not comply with the GDPR.

[62] The UN Trade and Development World consumer protection map provides relevant indicators and information on the status of consumer law and policy worldwide. In 2022, the WGE produced a report on Cross-border cooperation: https://unctad.org/system/files/information-document/ccpb_E-Commerce_Cross_Border_Report_Final_en.pdf

[63] See for example, the practice of 'algorithmic disgorgement', which includes cases taken on by the FTC in the United States of America and requiring the destruction of AI models reliant on data they are not legally allowed to use https://www.debevoisedatablog.com/2022/03/22/model-destruction-the-ftcs-powerful-new-ai-enforcement-tool/

[64] See for example, in the European Union, the provisions of the Artificial Intelligence Act.

[65] See for example, in the European Union the proposed the AI Liability Directive, at early stage of development, which would modernise the existing rules on the strict liability of manufacturers for defective products and provide redress to consumers harmed by AI systems, https://www.europarl.europa.eu/RegData/etudes/BRIE/2023/739342/EPRS_BRI(2023)739342_EN.pdf.

[66] Executive Order (30 October 2023) https://www.whitehouse.gov/briefing-room/presidential-actions/2023/10/30/executive-order-on-the-safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence/

[67] Executive Order (30 October 2023) Sec.2 (e).

to the report to Congress, which calls for caution to be exercised in the use of AI.[68]

In 2020 the FTC issued a set of guidelines on AI notably encouraging businesses to have regards to the robustness and soundness of data models, transparency, 'explainability' of decision making and fairness.[69] Businesses' engagements and compliance with basic rules on AI models is an important aspect of controlling practices and protecting consumers. AI use by businesses would benefit from clear guidelines that are currently lacking. In the United Kingdom, the Competition and Markets Authority (CMA) has also proposed some principles for the development and use of AI foundation models to guide competitive AI markets and protect consumers.[70] Those principles include accountability, access, diversity, choice, flexibility, fair dealing and transparency. These align with the five principles agreed by the UN Advisory Body on AI - detailed in the paragraph below- and serve as a sound basis for ethical business conduct in AI use. [71]

Toward global governance of AI.
Looking ahead, the UN Secretary-General's High-Level Advisory Body on AI has outlined a path toward global AI governance. To help address the current governance gap and ensure that the use of AI technologies does not cause undue harm to users and consumers, the Secretary-General has called for inclusive, rights-based, and accountable governance that "should integrate the private sector, civil society, independent scientists and all those driving AI innovation."[72]

Established in 2023, the Advisory Body developed five guiding principles to shape future international AI governance institutions. [73] These principles call for governance that is inclusive—developed by and for the benefit of all; oriented toward the public interest rather than narrow commercial goals; interlinked with data development and governance; universal and collaborative in nature; and firmly anchored in the United Nations Charter, international human rights law, and the Sustainable Development Goals.

As a concrete step forward, the UN AI Advisory Body called for the establishment of a dedicated AI office within the UN Secretariat to coordinate global initiatives. It also highlighted the need to address unchecked corporate power and ensure that consumer rights and fair competition are not compromised by the use of AI.

[68] https://www.ftc.gov/news-events/news/press-releases/2022/06/ftc-report-warns-about-using-artificial-intelligence-combat-online-problems

[69] https://www.ftc.gov/business-guidance/blog/2020/04/using-artificial-intelligence-algorithms, summarized and publicised in https://www.ftc.gov/business-guidance/blog/2021/04/aiming-truth-fairness-equity-your-companys-use-ai and https://www.ftc.gov/business-guidance/blog/2023/02/keep-your-ai-claims-check

[70] Foundation models are large deep learning neural networks. They are massive data sets used as a starting point to develop AI. CMA, AI Foundation Models: Initial Report (2023), https://www.gov.uk/government/news/proposed-principles-to-guide-competitive-ai-markets-and-protect-consumers

[71] https://www.ftc.gov/business-guidance/blog/2020/04/using-artificial-intelligence-algorithms, https://www.gov.uk/government/news/proposed-principles-to-guide-competitive-ai-markets-and-protect-consumers

[72] Secretary-General's remarks to the Security Council on Artificial Intelligence

[73] . AI Advisory Body, Governing Ai for Humanity, final report (September 2024) p.38. See: https://www.un.org/sites/un2.un.org/files/governing_ai_for_humanity_final_report_en.pdf

Chapter 5

Use of technology (including AI) by public consumer protection law enforcement agencies

The use of technology in enforcement settings is taking hold. There is clear potential for using AI and other technologies in both private and public enforcement. This section primarily focuses on public enforcement.

Harnessing AI to assist consumers in decision making. AI roll out can cause harm to consumers, but it can also assist them in making better choices or streamlining complicated processes.[74] For example, AI can be harnessed to assist consumers or alert of potential risks to avoid, thus pre-empting the need for private enforcement. There are many examples of technology being used to help users with various legal matters, such as cancelling subscriptions, disputing charges, navigating bureaucratic processes, and even providing legal assistance for refugees seeking asylum. One such example is an app that uses artificial intelligence to automate the process of generating legal documents and providing guidance to users. [75] AI can also be harnessed to help flag to consumers where dark patterns may be used, so that they can better avoid them as well as understand how and where they operate.[76] In India, the Government has been active in engaging with business and asking consumers to report wrong-doing.[77] More recently, the department of consumer affairs launched the dark pattern buster Hackathon 2023 to create an app or software that could assist consumers in detection of dark patterns.[78] The department envisages it will also use a similar tool in its own enforcement efforts. Consumer associations are also looking into ways of harnessing AI to help consumers.[79]

The use of technology in the public enforcement of consumer laws. Consumer agencies have started to embrace technological solutions (referred to as Enforcement Technology, or EnfTech for short[80]) including AI systems to help streamline and improve interventions. Given the environmental concerns and risks highlighted above, floating the prospect of using AI in consumer enforcement may be counter intuitive. Embracing technology to 'fight' technology in enforcement may not be desirable.[81] It may also fuel the debate on 'technological solutionism', i.e. the belief that any issue can be improved using technology while disregarding pressing social, cultural, and political root causes.[82]

However, the growing consensus is that enforcement agencies must leverage technological tools to keep pace with the increasing sophistication of industry practices. Failing to do so risks making enforcement less effective.[83] Given the speed and scale at which AI is being adopted in the private sector, enforcement agencies may no longer be able to rely solely on human resources and

Consumer protection agencies are increasingly using AI to detect violations, manage complaints, and enhance dispute resolution, allowing for more proactive and effective enforcement despite resource and institutional barriers.

[74] For example, Chat GPT can be used to subscribe to social media or unsubscribe to social media assisting consumers who may not be best versed in using IT tools (video WGE webinar 2 – minute 36:00 to 50:00).

[75] See for example www.donotpay.com.

[76] The Dark pattern highlighter developed by the Dapde project in Germany (https://github.com/Dapde/Pattern-Highlighter) is an open-source browser extension which helps users navigate the internet by highlighting common dark patterns used on websites. The tool does not block dark patterns, but simply highlights them so that consumers become aware of the influences affecting them and provides information about the type of pattern encountered.

[77] https://jolt.richmond.edu/2023/10/04/dark-patterns-and-indias-legal-battle-for-ethical-e-commerce/

[78] https://unctad.org/system/files/non-official-document/ccpb_WGE_Webinar__A1_India_en.pdf

[79] For example, the CICLE project feeds regular information collected by consumer associations to enforcement authorities to fill the gap in market surveillance and promote cooperation. The classification of complaints and data collected will be powered by AI from 2023 onwards to help streamline complaints and detect cross-border problems more efficiently.

[80] Introducing EnfTech: A technological approach to consumer law enforcement (2023) https://unctad.org/meeting/introducing-enftech-technological-approach-consumer-law-enforcement

[81] Federal Trade Commission, 'Combatting Online Harms Through Innovation; Federal Trade Commission Report to Congress' (2022) p.78.

[82] Norwegian Consumer Council, Ghost in the machine (June 2023) para 2.1.2., p.17.

[83] Riefa, Coll, The Transformative potential of Enforcement Technology (EnfTech) in Consumer Law (2024) p.15.

traditional methods to respond effectively, making this technological shift not just beneficial but increasingly unavoidable.

The transformative potential of technology in public enforcement.

The use of technology can be seen as potentially transformative, moving the work of consumer enforcement agencies from being largely ex-post to becoming more ex-ante and thus preventing harm before it occurs to the benefit of consumers.[84] The use of technology also has the potential to streamline enforcement processes and contribute to a faster reaction to infringements (using automatic analyses or data management for example). Technology can facilitate the redeployment of enforcement officers away from repetitive and time-consuming tasks[85] allowing them to focus on matters that need human input and lead to increase job satisfaction.[86] At the heart of this transformation is the question of how best to harness technology to serve the protection of consumers. The development and implementation of novel solutions require specific expertise and careful analysis of related hazards.[87]

For instance, Alternative Dispute Resolution (ADR[88]) and Online Dispute Resolution (ODR) mechanisms, enhanced by technologies like AI, chatbots, and blockchain, offer innovative ways to address consumer disputes effectively.[89] In ODR, AI can streamline processes by automating case management, analysing large datasets to predict outcomes, and improving accessibility through natural language processing.[90] Similarly, blockchain can ensure transparency and security in transactions, while chatbots can guide users through the dispute resolution process.

As highlighted in the UNCTAD report "Technology and the future of Online Dispute Resolution for consumer protection agencies" the adoption of ODR systems has already led to notable successes in the resolution of consumer complaints, such as Brazil's public platform Consumidor.gov.br.[91] As of September 2024, the platform has processed more than 8 million complaints, with over 1,500 registered businesses. Around 80 per cent of disputes were successfully resolved online between the consumer and the business and it took an average of within seven days. Emerging technologies also offer the opportunity to shift from reactive to proactive enforcement, minimizing harm to consumers before it occurs. For example, Poland's Office of Competition and Consumer Protection (UOKiK) uses an AI tool, ARBUZ, which helps national offices verifying unfair contract terms by analyzing standard contract provisions.[92] The UNCTAD report concludes that international collaboration and capacity-building are critical to developing scalable, accessible, and fair

[84] Riefa, Coll, The Transformative potential of Enforcement Technology (EnfTech) in Consumer Law (2024) p.16.

[85] Riefa, Coll, The Transformative potential of Enforcement Technology (EnfTech) in Consumer Law (2024) p.16. See also in the context of the use 'Technology and the Future of Online Dispute Resolution (ODR) Platforms for Consumer Protection Agencies' (UN Trade and Development 2023) where the potential of AI in enforcement is clearly identified, showing how AI can be useful for optimizing online consumer dispute resolution systems, and has potential to automate repetitive tasks and analyze large amounts of data, which can free up resources and improve efficiency in dispute resolution processes.

[86] Polish Office of Competition and Consumer Protection – UOKiK, White Paper, Advancing Consumer Law Enforcement with Artificial Intelligence (May 2024) p.5.

[87] Polish Office of Competition and Consumer Protection – UOKiK, White Paper, Advancing Consumer Law Enforcement with Artificial Intelligence (May 2024) p.5.

[88] Extrajudicial mechanisms. See UNCTAD Consumer dispute resolution in the World (UNCTAD/DITC/CPLP/2023/2) 19 Mar 2024.

[89] UN Trade and Development, Technology and the Future of Online Dispute Resolution (ODR) Platforms for Consumer Protection Agencies (2023)

[90] UN Trade and Development, Technology and the Future of Online Dispute Resolution (ODR) Platforms for Consumer Protection Agencies' (2023) p.13.

[91] https://www.consumidor.gov.br/pages/conteudo/sobre-servico

[92] See Polish Office of Competition and Consumer Protection – UOKiK, White Paper, Advancing Consumer Law Enforcement with Artificial Intelligence (May 2024) p.10

technology-based platforms. Efforts should focus on creating harmonized, open-source systems that address consumer rights while leveraging innovative technologies.

Choice of technologies to impact enforcement functions. Currently technologies can be used mostly for detection and to monitor/ gather evidence in consumer enforcement work, but it also has potential to be used in direct sanctioning activities.[93] Enforcement agencies can choose from a range of technologies and not simply AI. A study of the use of technology in consumer enforcement agencies found that gains can be made by agencies in all administrative set ups, and at all levels of technological development.[94] For example, agencies that have little resources can already benefit from concentrating on collecting data for future use[95] and using simple off-the-shelves tools to improve the efficacy of their interventions.[96]

In the EU, the eLab works with publicly available/ open-source tools that open access to data, such as domain name registries or national company registries, to give a risk score for any given entity based on provenance. This enables enforcers to target efforts where there are the most perceived risks.[97] The eLab also provides tools to conduct mystery shopping that mimic consumer behaviour but avoid detection, thus evading being blocked or given a different experience. A screen recording tool enables authorities to collect the evidence.[98] In Australia, the Competition and Consumr Commission (ACCC) uses an automated detection services to discover fraud, potential cyber-attacks, and frauds.[99]

Use of AI gathering pace in public enforcement. The adoption of AI is accelerating within enforcement agencies, although its implementation remains concentrated among a limited number of well-resourced consumer agencies. Compared to sectors like financial services or private industry, where AI is extensively utilized for regulatory purposes, consumer protection agencies are still in the early stages of integrating such technologies.[100] A significant barrier to widespread AI adoption in consumer enforcement is the lack of access to high-quality, structured data. As highlighted by EnfTech, this "data deficit" hampers the development and deployment of effective AI tools, particularly in agencies with limited resources. Moreover, agencies from developing countries, especially least developed countries (LDCs) are experiencing more fundamental challenges due to the digital gap, where billions are still offline. According to the UN Trade and Development Secretary-General, Rebeca Grynspan "*only 36 per cent of the population in least developed countries is online, and the gender gap in Internet use shows no sign of narrowing."101* She emphasised that "*AI will never be fair as long as over 3 billion people cannot access it"*.[102] AI comes to an already complicated situation where digital penetration

[93] Riefa, Coll, The Transformative potential of Enforcement Technology (EnfTech) in Consumer Law (2024) p.16.

[94] Riefa, Coll, The Transformative potential of Enforcement Technology (EnfTech) in Consumer Law (2024) p.73.

[95] https://www.enftech.org/blog/data-deficit-slows-down-ai-consumer-enforcement

[96] Riefa, Coll, The Transformative potential of Enforcement Technology (EnfTech) in Consumer Law (2024) p.19.

[97] Riefa, Coll, The Transformative potential of Enforcement Technology (EnfTech) in Consumer Law (2024) p.43.

[98] Riefa, Coll, The Transformative potential of Enforcement Technology (EnfTech) in Consumer Law (2024) p.42. Note that the Italian authority has reported using several types of software and tools (like web scrappers, emulators and smartphone simulator) that were provided in the framework of the EU lab during sweeps conducted in 2023.

[99] Riefa, Coll, The Transformative potential of Enforcement Technology (EnfTech) in Consumer Law (2024) p.47. The agency uses Netcraft.

[100] Riefa, Coll, The Transformative potential of Enforcement Technology (EnfTech) in Consumer Law (2024) p.61.

[101] ITU Facts and Figures 2023, Internet use: https://www.itu.int/itu-d/reports/statistics/2023/10/10/ff23-internet-use/

[102] Statement by Rebeca Grynspan, Secretary-General of UNCTAD, World Consumer Rights Day Debate Series organized by Consumers International, Fair and Responsible AI for consumers: https://unctad.org/osgstatement/world-consumer-rights-day-debate-series-organized-consumers-international

remains uneven. According to ITU Digital Development, "*uneven progress in global Internet connectivity highlights the disparities of the digital divide and is leaving people in low-income countries behind."103* In those countries use of AI in enforcement tasks will inevitably be more protracted and international collaboration will be of great use, to ensure a truly global governance of AI where no one is left behind.

Examples of the use of AI by consumer agencies to enforce consumer rights.

AI is already proving useful for several key and yet time consuming tasks, including reading documents, flagging potentially non-compliant materials, and making recommendations to enforcement officers. AI can be applied to detect and investigate influencer marketing, dark patterns, unfair terms, unfair commercial practices (like price discrimination, countdown, etc.)

The Authority for Consumers and Markets in the Netherlands has develop an accessible web scraper[104] which is designed to be easy for enforcement agency staff to use. This tool is AI-powered and includes automatic data capture and analysis features, making it easy to gather evidence on potentially unfair commercial practices.[105] The same authority has a tool capable of scanning spoken words in telemarketing phone calls to detect wrongdoing. The use of AI has enabled the scaling up of detection.[106]

INDECOPI, the Peruvian Consumer Agency, is also using AI to monitor spam telephone calls. This way, they have proved more efficient in being able to pinpoint if companies were complying with the law, which prohibits calls without prior consent. The use of AI has enabled the agency to expand their reach by being able to review many more practices than was possible with 'human only' investigations.[107]

In Poland for example, UOKIK, having launched an AI tool to detect unfair terms in consumer contracts in 2023[108], is now rolling out an AI programme for dark patterns with a project that should deliver a workable proof of concept prototype by 2026.[109] The first system, known as Arbuz, uses natural language processing to scan and analyze standardized contract terms, flagging potentially abusive provisions based on a legal database curated by the agency. Based on the success of the first tool, UOKiK is currently developing an AI-based dark pattern detection tool that identifies manipulative design features on websites, such as false scarcity messages, default opt-ins, and misleading countdown timers. To train this system, UOKiK combined technical website analysis with insights from psychological and neuromarketing research

In the Republic of Korea, the Korea Consumer Agency (KCA) has implemented a comprehensive AI-Based Knowledge Platform as part of a national digital transformation strategy. This platform integrates several AI-powered tools designed to improve complaint management and institutional efficiency. Key components include an internal search engine that retrieves relevant regulatory and case law information, and an AI-based drafting system that assists in preparing initial versions of dispute settlement decisions. Additionally,

[103] Facts and Figures 2023 publication https://www.itu.int/hub/publication/d-ind-ict_mdd-2023-1/

[104] A web scraper is a software tool that automatically scans and extracts data from websites.

[105] Riefa, Coll, The Transformative potential of Enforcement Technology (EnfTech) in Consumer Law (2024) p.42.

[106] Riefa, Coll, The Transformative potential of Enforcement Technology (EnfTech) in Consumer Law (2024) p.40.

[107] https://www.gob.pe/institucion/indecopi/noticias/951375-el-indecopi-inicia-fiscalizacion-por-llamadas-sin-consentimiento-o-spam-telefonico-aplicando-inteligencia-artificial

[108] UOKiK's AI tool ARBUZ helps control unfair contract terms by analyzing standard contract provisions and assisting employees in verifying their legality. ARBUZ conducts preliminary document analysis to identify potentially abusive terms that violate consumer rights. It compares contract fragments with previously identified abusive or safe clauses using a database of annotated excerpts from court rulings and UOKiK decisions. Continuously analyzing and updating the database through supervised machine learning, ARBUZ efficiently identifies and flags potentially abusive contract sections.

[109] Video to the UN Trade and Development WGE webinar on AI and consumer protection: harnessing tech to better enforce consumer law

KCA has developed a consumer-facing chatbot offering standardized responses to frequently asked questions.

In Thailand, the Office of the Consumer Protection Board (OCPB) has deployed AI tools for automated complaint triage that filters and prioritizes complaints based on severity and subject matter, improving case management efficiency. OCPB also operates an AI system to detect fraudulent digital advertising, which scans online platforms in real-time to flag misleading claims, particularly in health-related products and pricing promotions.

In Zambia, the Competition and Consumer Protection Commission (CCPC) has initiated AI integration through the development of a chatbot-enabled case management system and a market surveillance tool. The chatbot allows consumers to file and track complaints online, reducing reliance on in-person services. The market surveillance tool, still in development, aims to monitor digital marketplaces for price manipulation and collusive behavior.

The use of technology and in particular AI presents several challenges for agencies to work through.[110] One of the first will be determining if AI is in fact the best technology to adopt in the first place and avoid falling for the hype[111] around the potential benefits of this technology. Beyond this, consumer protection agencies face operational, legal, and cultural barriers. Data limitations are a major concern, as AI requires large quantities of high-quality, structured data to function effectively—something many agencies may lack.[112] Agencies may also face an "arms race", where regulated businesses adopt more advanced tools to evade detection, requiring enforcement bodies to continually upgrade their systems just to keep pace.[113] Institutional resistance or a lack of digital skills among staff can further hinder implementation, requiring significant investment in training and culture change. Legally, existing frameworks may not yet accommodate AI-driven enforcement, raising questions about transparency, fairness, and liability, particularly when agencies rely on third-party AI models whose workings they cannot fully audit or explain.[114] Finally, AI's opacity and risk of bias may undermine trust if consumers or businesses view decisions as arbitrary or discriminatory.

[110] The below is not an exhaustive list but merely highlights some key issues. Other problems can be found listed notably in Riefa, Coll, The Transformative potential of Enforcement Technology (EnfTech) in Consumer Law (2024); AI Advisory Body, Governing Ai for Humanity, interim report (December 2023) https://www.un.org/sites/un2.un.org/files/ai_advisory_body_interim_report.pdf; Polish Office of Competition and Consumer Protection – UOKiK, White Paper, Advancing Consumer Law Enforcement with Artificial Intelligence (May 2024)

[111] Riefa, Coll, The Transformative potential of Enforcement Technology (EnfTech) in Consumer Law (2024) p.68.

[112] UN Trade and Development, Technology and the Future of Online Dispute Resolution (ODR) Platforms for Consumer Protection Agencies (2023) p.14.

[113] Riefa, Coll, The Transformative potential of Enforcement Technology (EnfTech) in Consumer Law (2024) p.68.

[114] Riefa, Coll, The Transformative potential of Enforcement Technology (EnfTech) in Consumer Law (2024) p.67-68.

Chapter 6

Quality data for quality AI tools

Quality data is a key consideration in the use of AI for public consumer law enforcement. AI can be good at several tasks, but to do so, it requires large amounts of good quality data that consumer agencies may not yet possess or to which they do not have access.[115] AI models can be biased by the data used for their training, and AI systems may produce incorrect results due to discrepancies between their language generation capability and knowledge.[116] In agencies starting their journeys towards more use of technology, efforts may first need to focus on building data sets.

Data curation and analysis begin with the collection and organization of diverse and representative data relevant to the agency's activities, such as records of market practices, consumer complaints, business compliance data, or enforcement actions. Once collected, the data must be pre-processed, including cleaning, structuring, and standardizing it to ensure it is fit for AI analysis. This process involves handling missing information, converting data into usable formats, and removing errors or irrelevant content. Finally, through exploratory data analysis, agencies can examine the data to identify trends, patterns, and relationships that support more informed decision-making and the development of reliable AI-powered tools for monitoring, enforcement, or policy design.[117]

More advanced agencies may wish to reflect on the quality of their data and look into processes to harness the data currently held to help make prioritization choices.[118] Data that is 'clean' [119]is a pre-requisite to avoid risks such as discrimination and bias and thus requires investments in preparing data sets before AI can be used as a reliable tool. In Poland, UOKiK's AI tool ARBUZ helped the building of diverse and organized data sets to help the AI accurately interpret complex contexts, such as the legal environment.[120]

There is a risk of legal challenge if businesses and practices identified by the technological tools lead to unfair sanctioning. At present, agencies seem to have pre-empted those issues, in large part because technology is an aid to enforcement officers who then review flagged practices manually. AI should be seen as a tool to assist humans in enforcement work, enhancing efficiency and effectiveness, rather than as a replacement for human judgment and oversight. As more efficiencies are baked into the system the risks of bias and discrimination in enforcement practices may grow and thus should be kept under close review. Similarly, despite good data being used, AI systems can also lead to skewed identification of problems, issues around correlation and causation and linked with the way the AI may imply results from the data it ingested.

The effectiveness of AI tools in enforcement depends on access to high-quality, well-structured, and representative data, requiring agencies to invest in data preparation, governance, and ongoing quality assurance.

[115] Riefa, Coll, The Transformative potential of Enforcement Technology (EnfTech) in Consumer Law (2024) p.69.

[116] UN Trade and Development, Technology and the Future of Online Dispute Resolution (ODR) Platforms for Consumer Protection Agencies (2023) p.14.

[117] UN Trade and Development, Technology and the Future of Online Dispute Resolution (ODR) Platforms for Consumer Protection Agencies (2023) p.14.

[118] Similar problems are magnified when using generative AI and foundation models that rely on massive data sets as a starting point to develop AI. See CMA, AI foundation models – Update paper (11 April 2024), https://assets.publishing.service.gov.uk/media/661941a6c1d297c6ad1dfeed/Update_Paper__1_.pdf

[119] Clean data refers to information that is accurate, complete, well-structured, and free from errors or irrelevant content.

[120] Polish Office of Competition and Consumer Protection – UOKiK, White Paper, Advancing Consumer Law Enforcement with Artificial Intelligence (May 2024) p.11.

Chapter 7

Enhancing the technological capacities of consumer protection agencies

In many respects, even in countries where a regulatory framework is in place or developing at pace, agencies may not yet be geared to control the harm caused by AI. Expertise and resources are needed[121] to understand industry practice, conduct investigations and think of solutions and sanction wrongdoing. Rolling out AI and other innovative technologies in consumer enforcement requires staffing and resources that may currently be beyond the reach of most consumer agencies, especially in developing countries. The recruitment and retention of technologists amidst the ranks of enforcement officers, policy specialists, lawyers and economists already working in consumer agencies is pivotal key in building capacities.

Training existing staff is also essential for success, as all enforcement officers may eventually need to use technological tools in their work or contribute to their development. While AI-driven automation has the potential to affect certain jobs, current experience suggest that it has mostly enhance the work of enforcement officers rather than replace human input.[122] Training is important but requires resources. According to the UNGCP, Member States should ensure that consumer protection enforcement agencies have the necessary human and financial resources to promote effective compliance.[123] Yet, many agencies face significant barriers, including inadequate technological infrastructure and limited budget. Without access to computers, fast internet and storage systems, deploying AI effectively may prove extremely difficult.

Agencies must strengthen their technological capacities by investing in infrastructure, staff training, and multidisciplinary expertise to keep pace with evolving AI challenges and ensure fair and efficient consumer protection.

[121] For example, in the United States of America, Executive Order (30 October 2023) requires the appointment of chief technologist in all agencies of US. In Italy, the government has announced tax relief schemes to attract AI talent to Italy.

[122] Poland has adopted the approach of building a team based on a matrix structure, where members from specialized departments, including computer science, data analysis, law, human resources, and finance collaborated in the project. This method offers flexibility, efficient resource allocation, and supports open communication within the organization, enhancing team responsiveness. UOKiK's experience confirms its effectiveness. See Polish Office of Competition and Consumer Protection – UOKiK, White Paper, Advancing Consumer Law Enforcement with Artificial Intelligence (May 2024) p.10.

[123] UNGCP 15

Chapter 8

International cooperation

Adopting a collaborative and international approach to addressing consumer protection challenges, given the global nature of e-commerce.

AI deployment is generally costly. Costs include the price of new technologies but also integration with existing systems, employee training, and potential operational issues. Thus, exploring funding sources such as national and regional funds, and partnering with other institutions for knowledge exchange, is crucial. [124] For example, the UKiKO from Poland, took a collaborative approach when deploying their AI tools, emphasizing the importance of leveraging available funding and partnerships to support the development and implementation of new technologies. Agencies may therefore well want to pull resources together to develop tools that could then be used by all to tackle similar tasks.[125]

Recent global initiatives underscore the increasing emphasis on international cooperation and capacity building to ensure equitable AI deployment. In March 2024, the General Assembly adopted a Resolution on seizing the opportunities of safe, secure, and trustworthy artificial intelligence systems for sustainable development.[126] This Resolution aims to foster the development and utilization of AI systems. It calls for global cooperation to create standards and frameworks that enable equitable sharing of AI benefits, focusing on aiding developing countries. Additionally, it supports capacity, technical, and financial assistance to developing countries to enhance their participation in AI advancements and governance. Further, in June 2024, the General Assembly adopted a resolution that calls upon the United Nations system to enhance action-oriented international cooperation on artificial intelligence capacity-building, including cooperation frameworks or initiatives, to promote the participation of developing countries in artificial intelligence processes.[127] Similarly, the UN Secretary-General's High-Level Advisory Body on AI has recommended the establishment of a global capacity development network and a dedicated AI fund to bridge the digital divide.[128] These initiatives echo the commitments made in the Pact for the Future, calls for enhanced international cooperation and stakeholder engagement to manage risks and promote an inclusive, responsible, and sustainable digital future. The Pact includes a Global Digital Compact,[129] which sets the enhancement of international AI governance as one of five objectives to achieve a fair, safe, and secure digital future for all.[130] Objective 5 underscores the need for balanced, inclusive, and risk-based governance, with full participation from all Member States, especially developing countries. It also highlights AI's potential to accelerate progress on the Sustainable Development Goals (SDGs), advocating for governance that supports diverse cultures and languages and prioritizes locally generated data.

> International collaboration, knowledge sharing, and joint tool development are essential to enable all countries- especially developing countries- can leverage AI safely and equitably in consumer protection.

[124] European initiatives like eLab provide platforms for digital tool development and can drive public sector innovation through collaboration and external funding.

[125] For example, in the United Kingdom, see the Digital Regulation Cooperation Forum which will act as a focal point for collaboration amongst regulatory agencies in the United Kingdom including the Competition and Markets Authority (CMA), the Office of Communications (Ofcom), The Information Commissioner's Office (ICO) and the Financial Conduct Authority (FCA). See, DCFR Work Plan 2024/2025 (April 2024) https://www.drcf.org.uk/__data/assets/pdf_file/0030/283188/DRCF-Workplan-202425.pdf

[126] A/78/L.49

[127] A/78/L.86

[128] AI Advisory Body, Governing Ai for Humanity, final report (September 2024) p. 64. See: https://www.un.org/sites/un2.un.org/files/governing_ai_for_humanity_final_report_en.pdf

[129] United Nations Pact for the Future, Global Digital Compact and Declaration on Future Generations (September 2024) p. 40. See: https://www.un.org/sites/un2.un.org/files/sotf-the-pact-for-the-future.pdf

[130] The Global Digital Compact, as outlined in the *Pact for the Future* (Annex I), identifies five key objectives: (1) Connect all people to the Internet, including schools; (2) Respect human rights in digital contexts; (3) Introduce accountability for discrimination and misleading content; (4) Promote regulation of artificial intelligence; and (5) Foster a digital commons as a global public good.

Collectively, these developments reinforce the urgency of supporting underserved regions through international partnerships, resource sharing, and the creation of interoperable standards—areas where UN Trade and Development plays a pivotal facilitating role.

To protect consumer efficiently, there is a need to stimulate cross-agency collaborations and sharing of best (and worse) practices to enable accelerated learning across agencies.

In this sphere, international collaborations and exchange of knowledge and best practices would be paramount to learn from positive implementation stories as well as reflect on necessary improvements. Intensifying the exchange of experiences between countries, using UN Trade and Development as facilitators would thus be of great value to consumer agencies, while recognizing that bilateral cooperation also plays a crucial role in technology transfer. UN Trade and Development's role is particularly valuable as it works with member States at various levels of development. It is important to consider these varying levels, as by fostering tailored and inclusive cooperation, the benefits of technology transfer can be maximized for all.

Develop best practice in the deployment of AI in consumer law enforcement agencies. AI deployment raises ethical and procedural issues. Agencies will have to approach AI with a critical eye to ensure it is employed safely and effectively, which requires referencing best practices and adhering to a set of principles for fair use of technology in enforcement. It may be beneficial to reflect on how the United Nations Guidelines on AI[131] will apply in the context of consumer protection and define 'best practice' parameters for agencies engaging in the use of AI for enforcement purposes.

[131] https://www.un.org/en/ai-advisory-body

Chapter 9

Conclusions and suggestions for action to governments and consumer protection agencies

AI offers transformative opportunities for both consumers and consumer protection agencies. For consumers, AI-driven tools can enhance convenience, improve access to tailored services, and facilitate better informed decision-making. Personalized recommendations, automated assistants, and real-time fraud detection systems empower consumers to navigate digital marketplaces with improved transparency and accessibility. Concerning consumer protection law enforcement, consumer protection agencies are increasingly leveraging AI to enhance market surveillance, detect unfair commercial practices, and automate dispute resolution processes. The AI-powered tools mentioned in the report showcase how some enforcement authorities are effectively deploying AI to proactively protect consumers from manipulative business practices.

Despite these benefits, AI poses significant risks to consumers. A major concern is the opacity of AI decision-making and the difficulty in holding businesses accountable for harmful or biased AI-driven outcomes. Many AI systems operate as black boxes, making it difficult for consumers to understand the results with which they are presented. This lack of transparency can exacerbate discrimination and bias, particularly against vulnerable consumer groups. In financial services, for example, AI-driven credit scoring models have been found to disadvantage minority groups due to embedded biases in training data.

Another critical challenge is AI's impact on competition in markets. The AI sector is increasingly dominated by a handful of multinational technology firms that control key components of the AI value chain, including cloud computing, data infrastructure, and foundational AI models. The current AI oligopoly allows major players to shape markets to their interests. Additionally, algorithmic pricing and AI-powered market monitoring tools increase the risk of collusion, allowing dominant firms to engage in tacit price coordination without explicit agreements.

Consumer privacy is another area of growing concern. AI models, particularly in digital advertising and social media, thrive on large-scale personal data collection. Many consumers remain unaware of how their data is being harvested, processed, and monetized by AI-driven platforms. Additionally, AI-generated content and deepfakes are becoming increasingly sophisticated, making it harder for consumers to distinguish between truthful and manipulated information. AI-powered scams and fraudulent schemes, such as highly realistic phishing emails and audio deepfakes, pose a direct threat to consumer safety. On the other hand, public data represents a valuable source of evidence for enforcement agencies.

Environmental sustainability is another growing concern associated with AI. The development, training, and deployment of AI models require significant computing power and energy consumption, contributing to the carbon footprint of digital industries. AI models, particularly large language models and deep learning systems, require vast amounts of electricity for both training and operation.

As AI continues to shape digital markets, consumer protection agencies are adapting their enforcement strategies to leverage technological advancements. By integrating AI-driven tools into their daily, agencies can improve market surveillance, detect unfair business practices more efficiently, and enhance enforcement capabilities.

As shown throughout the report, consumer protection agencies are actively integrating emerging technologies to safeguard consumer rights These initiatives demonstrate how AI can serve as a tool for enforcement agencies to mitigate risks and enhance consumer rights protections.

At the international level, international organizations and governments are working to develop AI governance frameworks that align with consumer protection principles.

> Harnessing AI for consumer protection requires a holistic approach that combines ethical regulation, innovation, education, and cooperation, ensuring AI serves consumer empowerment, not harm or misuse.

However, regulatory efforts remain uneven across countries, particularly in developing countries, where limited resources, technical expertise, and regulatory infrastructure pose challenges in effectively governing AI markets. To tackle these challenges, consumer protection agencies rely on international collaboration and technical assistance to enhance AI enforcement. Partnerships among regulators, academia, and the private sector could help develop enforcement tools and build AI literacy.

These conclusions highlight the pressing need for tailored, international cooperation to address the challenges and unlock the full potential of AI for consumer protection.

As shown in this report, harnessing AI responsibly will require a multifaceted approach involving the development of ethical guidelines, capacity building, and international cooperation. The following suggestions aim to provide practical steps for governments and consumer protection agencies to navigate the complexities of AI responsibly, addressing its risks while leveraging its potential to advance consumer welfare.

In the context of the conclusions of this report, consumer protection agencies and policymakers may wish to consider the following suggestions:

Suggestions for action to consumer protection agencies

Adopt and promote best practices: While AI offers powerful tools to enhance enforcement capabilities, its deployment should align with international best practices and ethical standards to ensure fairness, transparency, and accountability. By adopting well-defined principles and promoting responsible business conduct, regulators can strengthen oversight, improve consumer trust, and create a more balanced digital marketplace.

- Align the promotion of high-quality AI tools with the UN Global Digital Compact.[132] The most relevant objectives for consumer protection being: fostering an inclusive, open, safe, and secure digital space that respects human rights; expanding inclusion in and the benefits of the digital economy for all; and advancing responsible, equitable, and interoperable data governance approaches.
- Promote the adoption of regulations and guidelines that encourage ethical business practices in the use of AI in business-to-consumer (B2C) relationships.

Boost consumer education: As AI technologies reshape digital markets, many consumers remain unaware of how these technologies influence their choices, personal data, and marketplace interactions. From manipulative dark patterns to AI-generated scams, these risks can erode trust and expose consumers to unfair practices. Strengthening consumer education is crucial to improving digital literacy, empowering individuals to recognize manipulation, and ensuring a fairer marketplace.

- Lead initiatives to inform consumers about AI risks and manipulation tactics, empowering them to identify and avoid unfair practices where possible.

Enhance technological capacities: As AI driven business practices

[132] The Global Digital Compact's five key objectives: (1) Connect all people to the Internet, including schools; (2) Respect human rights in digital contexts; (3) Introduce accountability for discrimination and misleading content; (4) Promote regulation of artificial intelligence; and (5) Foster a digital common as a global public good.

become more sophisticated, consumer protection agencies must advance their enforcement tools to effectively address emerging challenges. Strengthening technological capabilities and staff training will enhance monitoring, improve the detection of AI-driven manipulations, and optimize evidence gathering, enabling agencies to more effectively safeguard consumer rights in digital markets.

- Invest in emerging technological tools (including AI) and staff training to better monitor, detect, and address unfair practices in e-commerce, ensuring agencies are equipped to handle AI-driven challenges.

Foster international cooperation: With the expansion of AI-driven markets worldwide, international cooperation is vital for effective consumer protection. Many countries, especially developing economies, face challenges in regulating AI due to resource and expertise gaps. Collaboration allows agencies to share knowledge, develop enforcement tools, and align regulatory approaches, ensuring stronger consumer safeguards and harmonized AI standards.

- Engage in bilateral, regional, and global partnerships to share knowledge, tools, and best practices, aiming for coherent AI regulations and unified consumer protection efforts.

Suggestions for action to policymakers

Encourage the development of inclusive AI governance frameworks: Clear governance frameworks are essential to ensure the ethical use of AI, as emphasized in the Global Digital Compact (see 2. International context). Some governments have begun regulating AI or drafting national strategies. These efforts should align with consumer protection principles to prevent risks and promote fairness.

- Establish legal and regulatory frameworks that ensure AI development and deployment are ethical, transparent, and aligned with international legal norms.
- Align AI regulation with existing consumer protection frameworks.

unctad.org