ITUPublications

International Telecommunication Union
Development Sector

Output Report on ITU-D Question 6/1

Consumer information, protection and rights

Study period 2022-2025

Output Report on Question 6/1

Consumer information, protection and rights

Study period 2022-2025

Consumer information, protection and rights: Output Report on ITU-D Question 6/1 for the study period 2022-2025

ISBN 978-92-61-40931-9 (Electronic version)
ISBN 978-92-61-40941-8 (EPUB version)

Acknowledgements

The study groups of the International Telecommunication Union Telecommunication Development Sector (ITU-D) provide a neutral platform where experts from governments, industry, telecommunication organizations and academia from around the world gather to produce practical tools and resources to address development issues. To that end, the two ITU-D study groups are responsible for developing reports, guidelines and recommendations based on input received from the membership. Questions for study are decided every four years at the World Telecommunication Development Conference (WTDC). The ITU membership, assembled at WTDC-22 in Kigali in June 2022, agreed that for the period 2022-2025, Study Group 1 would deal with seven Questions within the overall scope of "enabling environment for meaningful connectivity."

This report was prepared in response to Question 6/1: Consumer information, protection and rights, under the overall guidance and coordination of the management team of ITU-D Study Group 1 led by Ms Regina Fleur Assoumou-Bessou (Côte d'Ivoire), as Chair, supported by the following Vice-Chairs: Mr Ali Rasheed Hamad Al-Hamad(Kuwait), Mr Amah Vinyo Capo (Togo), Mr George Anthony Giannoumis (Norway), Mr Roberto Mitsuake Hirayama (Brazil), Mr Sangwon Ko (Republic of Korea), Ms Umida Musaeva (Uzbekistan), Ms Caecilia Nyamutswa (Zimbabwe), Ms Memiko Otsuki (Japan), Ms Khayala Pashazade (Azerbaijan), Mr Sunil Singhal (India) and Mr Mehmet Alper Tekin (Türkiye).

The report was authored by the Co-Rapporteurs for Question 6/1, Ms Cristiana Camarate (Brazil) and Ms Wei Pei (China Institute of Communications), in collaboration with the Vice-Rapporteurs: Ms Hadiza Kachallah (Nigeria), Ms Lin Lin (People's Republic of China), Ms Tharalika Livera (Sri Lanka), Ms Caroline Kathure Murianki (Kenya), Ms Anne Chantal Ngondji (Cameroon), Mr Jesús Coquis Romero (Mexico), Mr Osman Sahin (Türkiye) and Mr Issouf Soulama (Burkina Faso).

Special thanks go to the chapter lead authors Ms Wei Pei (Introduction, Conclusion, § 3.3); Mr Issouf Soulama and Ms Tharalika Livera (Chapter 1); active collaborators Mr Daniel Araujo (Brazil) and Ms Elisa Daigele Bizarria (Brazil) with guidance from Ms Cristiana Camarate (Chapter 2); Ms Caroline Kathure Murianki (§ 3.1); Ms Hadiza Kachallah (§ 3.2); Ms Archana Gulati (§ 3.4); Ms Lin Lin (§ 4.1); Mr Osman Sahin (§ 4.2); Mr Jesús Coquis Romero (§ 4.3); Ms Anne Chantal Ngondji (Chapter 5); and active contributors Mr Teddy Woodhouse (United Kingdom), Mr Joseph Burton (United States) and Ms Nicola Bennett (Australia). This report has been prepared with the support of the ITU-D Question 6/1 focal points, the editors, the publication production team and the ITU-D Study Group 1 secretariat.

Table of contents

Executive Summary

This report contains the results of the study of ITU Telecommunication Development Sector (ITU-D) Question 6/1 (Consumer information, protection and rights) for the study period 2022-2025.

I. Background

The exponential growth of digital technologies and telecommunications services has transformed how consumers interact with markets, government services, and each other. The number of Internet users worldwide has doubled over the past decade, and is now estimated to stand at 5.5 billion. This shift has created new opportunities but is also a potential source of risks involving cybersecurity threats, online fraud, theft of personally identifiable information (PII), and exposure to deceptive marketing practices. Virtually universal Internet has made this a pervasive danger. National, regional and international bodies have acknowledged the urgent need for robust frameworks to protect consumers, particularly the most vulnerable groups and those from economically disadvantaged backgrounds.

This report is part of a broader initiative to identify successful regulatory practices and mechanisms that ensure digital inclusion, transparency, and consumer empowerment in the telecommunications and information and communication technology (ICT) sectors. It re-emphasizes the need for all stakeholders, especially governments, to support digital literacy initiatives, which play a crucial role in helping consumers navigate complex digital services and protect themselves from cyber risks.

This report is based on written contributions to the work of ITU-D Study Group 1 on Question 6/1 from participants representing ITU Member States, ITU-D Sector Members and Academia, and on the content of the following workshops: Trends in Consumer Protection Regulatory Instruments to Enable Digital Transformation,[1] held on 17 May 2023; Personal Data,[2] held on 17 April 2024; and Mechanisms to Promote Informed Consumer Decision Making,[3] held on 18 June 2024. Each chapter of this report provides specific guidelines on relevant topics based on the content mentioned above.

II. Main contents

The report comprises five chapters and highlights the importance of dialogue and regulation on digital consumer protection.

Chapter 1 emphasizes the need for comprehensive frameworks to empower and protect consumers in the digital age. It underscores the importance of coordination between stakeholders such as policy-makers, regulators, industry, and consumer associations in developing effective mechanisms for addressing consumer grievances and providing clear, accessible information.

---

1 https://www.itu.int/en/ITU-D/Study-Groups/2022-2025/Pages/meetings/session-Q6-1-may23.aspx
2 https://www.itu.int/en/ITU-D/Study-Groups/2022-2025/Pages/meetings/workshop-personal-data_april24.aspx
3 https://www.itu.int/en/ITU-D/Regional-Presence/Americas/Pages/EVENTS/2024/cons-awa-2024.aspx

Chapter 2 examines the current regulatory tools and policies used to ensure consumer protection. It stresses the need for these instruments to be fit for purpose, balancing consumer safety with the encouragement of innovation and competition. Further, it brings out the need for regulatory tools to be flexible and adaptable to dynamics in the ICT sector.

Chapter 3 delves into key issues regarding consumer protection in digital transformation, outlining strategies for safeguarding consumer interests while fostering the development of cutting-edge technologies including the Internet of Things (IoT).

Chapter 4 highlights the importance of providing consumers with clear, accessible information as a basis for informed decision-making. It discusses regulatory mechanisms such as transparency requirements, consumer education initiatives, and tools that help consumers compare services and understand the terms and conditions, empowering them to navigate digital services safely and confidently.

Chapter 5 highlights country-specific measures to protect vulnerable groups, such as older persons and persons with disabilities, through tailored regulations, accessibility initiatives and targeted education. These efforts aim to ensure inclusive, equitable access to digital services while enhancing overall consumer protection.

III. Key findings

Need for coordinated regulatory action: Consumer protection in the digital age requires coordinated efforts between governments, regulators, industry and consumer associations to develop effective frameworks that address the unique challenges posed by misuse and the proliferation of digital services.

Importance of fit-for-purpose regulations: Regulatory instruments must be tailored to address specific issues without stifling innovation. Regulations should strike a balance between protecting consumer rights and interests and encouraging market competition, innovation and technological progress.

Digital literacy as a pillar of consumer empowerment: Enhancing consumer awareness and digital literacy is crucial to protecting consumer rights and interests. Education and empowerment initiatives should focus on ensuring that consumers understand their rights, recognize fraud and know how to safeguard their PII.

Inclusive consumer protection frameworks: Effective consumer protection must take into account the needs of vulnerable populations, including individuals with disabilities and those from underserved communities. Policies must ensure that digital services are accessible to all, regardless of demographic factors.

Strengthening accountability and transparency: Service providers should be required to disclose clear, accessible information about their services and privacy policies. Transparency and interactive digital tools such as service comparison platforms foster trust and empower consumers to make informed decisions when purchasing, using, updating and terminating digital services.

Adaptability to emerging technologies: As new technologies like IoT and artificial intelligence (AI) reshape the digital landscape, consumer protection frameworks must evolve to address the

associated risks. Continuous monitoring and adaptation of regulations are necessary to keep pace with technological advancements.

International collaboration: The global nature of digital commerce and communications necessitates international collaboration to address cross-border issues such as online fraud, nuisance communications and data breaches. Sharing best practices and strengthening regulatory cooperation is essential.

Mechanisms for consumer redress: Effective mechanisms for lodging complaints and resolving disputes are central to consumer protection. Regulatory bodies should establish clear channels for consumers to voice their concerns and should ensure issues are resolved fairly and promptly.

Data protection safeguards: The protection of PII remains a critical concern in the digital economy. Regulatory frameworks should prioritize the security of consumers' personal data, establishing stringent guidelines for data handling and requiring organizations to implement effective safeguards.

Focus on ethical business practices: Businesses should adopt ethical marketing and data-collection practices to build consumer trust. Regulatory oversight can ensure that service providers adhere to fair practices, particularly in the use of consumer data for commercial purposes.

Abbreviations

Abbreviation	Term
2G/3G/4G/5G/6G	second/third/fourth/fifth/sixth-generation mobile communications[4]
ACCC	Australian Competition and Consumer Commission
ACMA	Australian Communications and Media Authority
AI	artificial intelligence
Anatel	National Telecommunications Agency (Brazil)
ARPTC	Post and Telecommunications Regulatory Authority of the Democratic Republic (the Congo)
ARTCI	Telecommunications/ICT Regulatory Authority of Côte d'Ivoire
AR/VR	augmented and virtual reality
BTK	Information and Communication Technologies Authority of Türkiye
CONATEL	National Telecommunications Council (Haiti)
IoT	Internet of Things
ITU-D	ITU Telecommunication Development Sector
ITU-R	ITU's Radiocommunication Sector
MNO	mobile network operator
NCC	Nigerian Communications Commission
NTRA	National Telecommunication Regulatory Authority (Egypt)
PII	personally identifiable information
RIFEN	International Network of Women Digital Experts
TIO	Telecommunications Industry Ombudsman (Australia)
TRCSL	Telecommunications Regulatory Commission of Sri Lanka
VAS	value-added service

[4] While care was taken in this document to use the official definition of IMT generations (see Resolution ITU-R 56, on naming for international mobile telecommunications), ITU-D would like to note that parts of this document contain material provided by the Membership referring to the common market designations of the form "xG". This material cannot always be mapped to a specific IMT generation, as the underlying criteria used by the Membership are not known. In general, IMT-2000, IMT-Advanced, IMT-2020 and IMT-2030 are referred to as 3G, 4G, 5G and 6G, respectively. Earlier technologies such as GSM, EDGE and GPRS are referred to as 2G by the market and could be considered as "pre-IMT" or "pre IMT-2000" technologies in ITU documentation and regulation.

Chapter 1 – The importance of dialogue on digital consumer protection

The digital landscape is rapidly evolving as new technologies, platforms and business models emerge. Ongoing dialogue helps ensure that consumer protection keeps pace with these changes and addresses emerging risks.

Empowering and protecting digital consumers has become an important part of the role played by policy-makers, regulators and consumer associations.

However, in order for the protection of consumer rights and interests to be full and effective, these different actors must work together and choose appropriate tools and instruments to inform consumers or address their complaints.

To achieve this objective, stakeholders must cooperate and exchange information and thereby align the mechanisms and tools for gathering consumer feedback and resolving consumer complaints.

1.1 Cooperation and information exchange among policy-makers, regulators and consumer associations

Protecting consumer rights and interests requires a structured system in which policy-makers, regulators and consumer rights associations collaborate closely. This cooperation is vital for effective consumer protection, ensuring that the needs of digital consumers are considered in policy and regulatory development. Globally, 67.5 per cent of ICT regulators are responsible for supporting consumer representation.[5]

In line with Resolution 64 (Rev. Kigali, 2022) of the World Telecommunication Development Conference (WTDC), on protecting users/consumers of telecommunications and ICT services, some countries have established collaborative frameworks to support digital consumers.

In Côte d'Ivoire,[6] Decision No. 2022-0723 of the Telecommunications/ICT Regulatory Authority (ARTCI) on 1 March 2022 established the Consumer Council. This committee is comprised of thirteen permanent members: nine representatives from consumer associations and four ARTCI officials. It serves as an inclusive platform for all stakeholders involved in protecting the consumers of telecommunication/ICT services. The committee's responsibilities include formulating opinions, proposing draft decisions and making recommendations to the ARTCI Regulatory Council on matters such as the protection of consumer rights, electronic transactions, personal data, and the prevention of cybercrime. Consumer association members are appointed for renewable two-year terms, following a transparent selection process defined by the ARTCI Regulatory Council.

[5] ITU Data Hub https://datahub.itu.int/data/?i=100039&s=3124
[6] ITU-D Document https://www.itu.int/md/D22-SG01.RGQ-C-0042/ from Côte d'Ivoire

Similarly, in Burkina Faso,[7] the Regulatory Authority for Electronic Communications and Posts (ARCEP) has established a consultation framework with consumer associations. This platform facilitates ongoing dialogue and information exchange with associations defending consumer interests, with a view to gathering their concerns and expectations regarding public initiatives for consumer rights protection. Unlike the Ivorian model, this framework is not codified in a legal instrument and typically convenes in workshops focused on specific themes, involving all legally constituted consumer associations.

In the Democratic Republic of the Congo,[8] the Postal and Telecommunication Regulatory Authority (ARPTC) has established collaboration mechanisms with consumer associations to enhance consumer protection in telecommunications and ICT services. These initiatives aim to address shortcomings in the customer service provided by mobile network operators (MNOs). The collaboration focuses on informing consumers about current ICT trends, identifying the challenges they face and providing information on available solutions. To implement this collaboration, ARPTC identified three consumer associations, one of which specializes in the ICT sector.

In Côte d'Ivoire,[9] public authorities are establishing permanent local centres to enhance consumer rights within the expanding digital ecosystem. These centres, strategically located across the country, aim to improve information dissemination and handle consumer complaints. This initiative seeks to foster trust between consumers and administrative bodies, promoting a more reliable digital environment.

1.2 Mechanisms/tools for receiving consumer feedback and resolving consumer complaints

To effectively protect consumers' rights, it is essential to establish legal systems or technical mechanisms that enable the timely receipt and resolution of complaints. According to the ITU Datahub, 85.3 per cent of ICT regulators globally are directly responsible for consumer complaint handling. Recognizing this need, many ITU Member States have implemented tools to gather feedback from consumers and address their complaints. While specific solutions vary across countries, the common goal is to empower consumers and the organizations dedicated to defending consumer rights, thereby ensuring that consumer concerns are heard and effectively addressed.

In Türkiye,[10] the Information and Communication Technologies Authority (BTK) has established an online complaint notification system to address consumer complaints related to electronic communication and postal services. This system allows consumers to submit complaints electronically, which BTK forwards to the relevant service providers for resolution. The system offers several advantages, such as paperless operation, a range of appeal opportunities, an effective complaint resolution system, regulatory insights and fast response times. This system empowers consumers and contributes to a more efficient and responsive digital services environment in Türkiye.

---

7 ITU-D Document https://www.itu.int/md/D22-SG01.RGQ-C-0052/ from Burkina Faso
8 ITU-D Document https://www.itu.int/md/D22-SG01.RGQ-C-0031/ from the Democratic Republic of the Congo
9 ITU-D Document https://www.itu.int/md/D22-SG01.RGQ-C-0056/ from Côte d'Ivoire
10 ITU-D Document https://www.itu.int/md/D22-SG01.RGQ-C-0089/ from Türkiye

The Nigerian Communications Commission (NCC) has implemented several initiatives to protect digital consumers, focusing on complaint resolution and consumer engagement.[11] The first tool is complaint channels, through which NCC provides a platform for consumers to submit unresolved complaints. These complaints are escalated to service providers with specified resolution timelines, ensuring timely responses. The second is consumer engagement, where NCC conducts various programmes to maintain dialogue with digital consumers, such as the Telecom Consumer Parliament. Another programme, Telecom Consumer Conversations, itself consists of various interactive programmes including: the Telecom Campus Conversation, a forum held at universities across the country where the regulators and service providers come together to educate tertiary students on salient industry issues and resolve their complaints; National Youth Service Corps Camp Sensitization, where the regulators educate camp participants on burning industry issues; Village Square Dialogue, a programme specially conceived for sensitizing telecom consumers at the grass roots level, delivered in the local languages; and Market Conversation, a programme for educating market vendors across the country on salient industry issues and their rights and privileges using language they understand. Through these initiatives, NCC strives to empower consumers, ensuring they are well informed and their concerns are effectively addressed.

In the Democratic Republic of the Congo,[12] ARPTC has prioritized consumer protection by establishing various collaboration mechanisms with consumer associations. These frameworks allow consumers' concerns and expectations about digital services to be raised and addressed. As a result of these collaborations, several tools have been created to better protect consumer rights, including the Central Equipment Identity Register (CEIR) system to combat mobile terminal theft and counterfeiting, and a web portal for consumers to submit complaints and compare services. This website also serves as a price simulator and comparator to allow users to view the offers available on the market, choose the ones best suited to their needs, and assess the budget to allocate to telecommunications services. One of the tools designed in collaboration with consumers is a toll-free line that collects complaints from consumers of digital services. ARPTC plans to further enhance this collaboration with initiatives like a Facebook discussion forum, a tripartite charter with MNOs and consumer associations, and periodic surveys to assess consumer satisfaction with telecom services.

In Australia,[13] the Telecommunications Industry Ombudsman (TIO), a free and independent alternative dispute resolution body for small business and residential consumers, has been established under the Australian Consumer Law and the Telecommunications Consumer Protections Code. It is important to note that all telecommunications providers are required to join the TIO scheme. This mechanism allows consumers whose complaints have not been resolved through traditional complaint resolution mechanisms to submit their complaints to the TIO. After reviewing the complaint, the TIO can either order a provider to pay compensation or refer the matter to the telecommunication regulator, the Australian Communications and Media Authority (ACMA), or to the Australian Competition and Consumer Commission (ACCC), which enforces consumer law.

[11] ITU-D Document https://www.itu.int/md/D22-SG01.RGQ-C-0020/ from Nigeria
[12] ITU-D Document https://www.itu.int/md/D22-SG01.RGQ-C-0031/ from the Democratic Republic of the Congo
[13] ITU-D Document https://www.itu.int/md/D22-SG01.RGQ-C-0061/ from Australia

In Brazil,[14] Anatel, the national regulatory authority, is responsible for defending and protecting the rights of consumers of telecommunication services. Consumers can register service complaints using the *Anatel Consumidor* system via smartphone app, Internet, call centre, or in person at Anatel offices. Service providers have their own channels and tools for receiving and processing consumer complaints, including the providers' own websites, which can register and process, *inter alia*, information requests, complaints, service requests and termination requests; free call centres operating around the clock; and physical stores. Anatel also requires that companies with significant market power maintain, in addition to the aforementioned service systems, an ombudsman that serves as an appeal body for consumers who are dissatisfied with the treatment of their complaints. In line with its consumer-centred mission, Anatel is developing measures that focus on customers' experiences and protect the rights of telecommunication consumers. These measures include the use of AI for the qualitative analysis of complaints and the use of the messaging app as an official entry channel, bringing Anatel even closer to consumers.

In China,[15] the telecommunications industry is based on sustained ethics and standards. Its high quality finds its origins in the disciplined state telecom operators, which strive to educate the public on their user rights. These operators are tasked with optimizing market service initiatives to promote informed decision-making among consumers. China Mobile, the country's largest telecom operator, takes proactive measures, in accordance with the laws and bills in force, to provide consumers with adequate information so that they can make informed decisions. China Mobile also gathers consumer feedback through complaint hotlines and customer service. The end goal is to reach total consumer satisfaction by ensuring that all telecom consumers receive high-quality services and can continue making informed decisions. To that end, the China Consumers Association, a nationwide social organization that safeguards the legitimate rights of consumers, operates as a third party, accepting consumer complaints, conducting investigations, offering consultation services to consumers and supporting them in legal actions to protect their rightsIt exposes incidents that infringe upon consumer rights and interests. One of its most influential initiatives is the annual nationwide live broadcast known as the "3.15 Gala," co-organized with relevant government departments. This program publicly exposes incidents that violate consumer rights, thereby integrating social supervision with regulatory oversight. By drawing wide public attention, the event creates strong pressure on enterprises, particularly telecom operators and service providers, to conduct self-examinations, improve compliance mechanisms, and promptly resolve consumer concerns.

In Haiti,[16] the National Telecommunications Council (CONATEL) oversees the telecommunications sector to protect consumer interests. CONATEL has established a dedicated unit to monitor operators and address consumer complaints, including issues such as lost minutes and unsolicited advertising. This unit gathers the complaints through phone calls and on-site forms, processing this data according to established procedures with a view to ensuring that consumers receive high-quality service in line with the conditions of the operators' licence. Additionally, CONATEL advocates for the implementation of online public communication services to enhance accessibility for individuals with disabilities. Recognizing the advancements in haptic technologies—such as remote controls, voice announcements on public transportation and sound signals at pedestrian crossings—CONATEL supports initiatives that empower the Secretariat of State for Persons with Disabilities. One such initiative is the *RepareNet* programme,

[14] ITU-D Document https://www.itu.int/md/D22-SG01-C-0146/ from Brazil
[15] ITU-D Document https://www.itu.int/md/D22-SG01-C-0222/ from China
[16] ITU-D Document https://www.itu.int/md/D22-SG01.RGQ-C-0171/ from Haiti

which trains young persons with disabilities to repair phones, enabling them to earn an income and participate in the digital economy. These efforts reflect the commitment of Haiti to improving telecommunications services and ensuring inclusivity for all citizens.

The Federal Telecommunications Institute of Mexico[17] has introduced the Complaint Map to provide users with visual insights into complaints against service providers across various regions. By analysing data from the I am User system, it categorizes complaints based on service type, non-compliance issue, state and year, enabling users to make informed choices about service providers.

In Egypt,[18] the National Telecommunication Regulatory Authority (NTRA) has launched its interactive application MyNTRA to facilitate the process of offering telecom services to users and corporations via mobile phones without the need to contact the call centre or make personal visits to operators' branches. The MyNTRA mobile application has a number of online interactive services designed for users including the Complaint System, which allows users to escalate their complaints to NTRA and also to enquire about and track their complaints.

1.3 Best practices for coordination and dialogue on digital consumer protection

The following is a summary of best practices in terms of coordination and dialogue among different stakeholders:

- **Rules for collaboration among stakeholders:** Set up regulatory frameworks that will aid cooperation and information exchange among policy-makers, regulators, industry and consumer associations.
- **Listen to the consumers:** Set up different mechanisms for lodging consumer complaints, such as emails, web-based and online applications, social media, phone-based systems, and physical stores, and roll out various forms of consumer education.
- **Digital channels can expand the reach of dialogue:** Digitize complaints systems so that feedback is sent directly to service providers, thereby eliminating the use of paper and mail, which increases digital transformation processes and helps track compliance.
- **Establishment** of **centres:** In certain situations, it can be beneficial to set up permanent offices for consumer complaints in strategic locations across the country. These centres can focus on consumer education, address questions and receive complaints, and ultimately help build a closer relationship with the community.
- **Timelines for resolving consumer complaints:** Ensure predictability and respect for consumer needs and demands by establishing timelines for resolving complaints. The regulator and companies will create streamlined processes for analysing and fulfilling the agreement.
- **Enforcement:** Establish adequate regulatory enforcement measures to ensure service providers comply with rulings in favour of consumers.
- **Prioritization:** Ensure that service providers and regulators provide accessible ICT products and services to persons with disabilities and ensure easy access to complaint resolution mechanisms.
- **Availability of data on consumer complaints:** Use information tools, such as 'heat maps' showing the distribution of complaints about service providers, to empower users so they can benefit from the experience of others in choosing a provider.

[17] ITU-D Document https://www.itu.int/md/D22-SG01.RGQ-C-0184/ from Mexico
[18] ITU-D Document https://www.itu.int/md/D22-SG01.RGQ-C-0190/ from Egypt

Chapter 2 – Trends in consumer protection policies and regulation instruments

2.1 Regulatory instruments that are fit for purpose

Policy and regulatory tools should be used in a way that is proportionate and limited to what is essential to achieve public policy objectives. They should not unnecessarily restrict economic freedoms or innovation in the market they regulate. The regulatory tools used by national regulatory authorities must be fit for purpose and allow for intervention in the market to achieve public policy objectives while balancing regulatory compliance, promotion of innovation, competition and consumer protection.

An important issue for the regulator is how regulated enterprises act in relation to public policy objectives. This might influence the selection of appropriate regulatory tools and techniques, which can be made by following a systematic procedure that considers the viewpoints and experiences of the various parties involved, utilizing methods such as public consultations, requests for evidence, data gathering, analysis of grievances, and other instruments, including informal discussions.

Following an initial, comprehensive analysis of the market, specific regulatory concerns can be identified and prioritized, in this instance, consumer protection issues. In this diagnostic phase, the primary focus should be on collecting and analysing data and evidence in order to identify particular problems and rank them in order of importance within the context of the local environment.

Complaints from customers, for example, can be analysed to identify the regulatory issues that are most frequently encountered or those that have the most significant influence on customers. One aspect to consider is that the problem that receives the greatest number of complaints might not necessarily be the one that should be prioritized. There may be a more fundamental cause that, if addressed, might potentially reduce the number of complaints. This could be the case even if takes less effort to resolve the issue. For example, if there is a significant number of customer complaints regarding unlawful charges does not necessarily require action on the billing processes itself; rather, action might need to be taken regarding the manner in which businesses advertise their products to customers.

Regulators should take proactive steps to reduce the existing informational asymmetry surrounding the specific problem once said problem has been identified and prioritized. These steps include using data and analyses, soliciting information, collecting data, and engaging in dialogue with stakeholders (such as consumer protection associations, service providers and consumers). After a substantial amount of information has been gathered, it is possible to construct a clearly defined scope of work that includes objectives that are understandable to all parties involved. This will result in the prioritizing of activities and will encourage a focus on tangible outcomes.

The goal is to always have qualitative and quantitative indicators available, and to ensure that entities concerned to comply with the rules and regulations. Complaints, for instance, indicate the number, type and details of customer issues and concerns. Periodic inspections should always be included in the diagnosis process, when measuring the level of implementation, and in more comprehensive investigations of non-conformity or searches for non-conformity when monitoring does not produce the intended outcomes.

Once the data provides the necessary evidence, precise and intensive action may be carried out, and consumer satisfaction and indices should be consistently monitored. Additionally, the regulator must determine how consumers respond to the regulatory intervention that may have been implemented.

Regarding the monitoring and evaluation of the market, regulatory impact assessments, particularly those that focus on consumers, enable the review of the regulatory interventions in force. Adequate and well-tailored regulatory interventions require reliable data, stakeholder consultation and independent analysis. As regulators shape the markets they regulate, this process of gathering evidence, consulting stakeholders and analysing relevant indicators can lend legitimacy to the regulator's actions. This, in turn, can make regulators more effective at protecting consumer interests.

In order to achieve regulatory compliance and enhance service provision, certain regulators implement definitions and the reciprocal reinforcement of fines and incentives. Incentives are believed to be crucial and generally take precedence over penalties. However, all tactics should be used according to the requirements of the situation and there should not be a predefined approach. Past experience of this approach has demonstrated that regulatory involvement is beneficial and more successful when the actions and standards of the regulator are able to encourage enterprises operating within the sector to go in a particular direction and by providing guidance and corrections as required.

The development of more responsive regulations and the measurement of their efficacy are dependent on the availability of transparent tools and processes that have the ability to modify the behaviour of the regulated entities in favour of the objectives. The regulated entities should be regarded as participants in the regulatory process, but ideally in a more proactive manner. They should take on an increasing amount of responsibility, including the organization and structuring needed to achieve the desired results. The regulator not only supervises this process, but also plays a proactive role in directing this organization and ensures that the organization's agility and outcomes meet the requirements of society and customers.

The experience gained during this process has shown that incentives lead to greater agility and resource efficiency, better allocation of efforts, and, in particular, more durable solutions to issues. Service providers can also adjust, implement and adapt their processes, allowing them to resolve real societal and consumer demands. As a result, consumers can benefit from solutions without having to repeatedly appeal to service providers and regulatory authorities to have problems resolved. One way of organizing incentives is to prioritize the actions of entities according to the most pressing needs and issues. In the context of greater engagement by incentive-driven regulated entities, the regulator should create an enabling environment, provide appropriate guidance for compliance with regulations, and encourage members of the business community to engage in ethical activities. Therefore, incentives are not rewards for performing obligations; rather, they contribute to the formation of a favourable and secure

environment for compliance with rules and regulations, in which fines and other external consequences are not seen to be normal.

Within this context, the experiences that are outlined in the best practices below (§ 2.2) also point to aspects, such as the need to strengthen the internal monitoring of regulated entities. The utilization of control through goals and indicators instead of continuous inspections, would reduce the information burden on regulated entities. This is also aligned with the demands for transparency and accountability, which come from both the regulated entities and the regulatory authority itself. Rather than merely reporting the activities and procedures that were carried out, the role of the authority and the entities should be noted with regard to the results achieved and the benefits that were provided to society. Although it may not be possible or desirable to foresee a single rigid flow, it is acknowledged that the common visualization and construction of a repertoire of tools is a very relevant task for the continuity and strengthening of responsive activities.

First and foremost, the problem-solving process should be open to the input of all stakeholders as much as possible, so that it can meet the current real demands of consumers and society, while also considering the internal perspectives of companies with regard to possible challenges and feasible changes. The goals of the process must be clear to all stakeholders. This clarity ensures the proper alignment of efforts and helps achieve the desired results. The purpose of the measures adopted should also be fair and proportionate to the intended response, and the possibility of more significant and impactful measures, as needed, should also be clear.

To assess the success of the initiatives and outcomes, it is important to establish and define indicators that demonstrate whether the regulatory interventions are capable of alleviating consumer difficulties and addressing societal concerns. Therefore, it is recommended to provide qualitative and quantitative indicators that measure the impact of the demands on the companies. For instance, consumer complaints indicate difficulties faced by consumers. Periodic inspections should be considered if the ongoing monitoring does not achieve the desired results.

In the course of responsive regulation, adjustments can be made throughout the processes, with the help of tools, in accordance with the characteristics and relevance of the issues, the conduct and responses of the regulated entities, and the outcomes presented. Such adjustments support the satisfactory resolution of the problems identified and improve services. The results should be disseminated and communicated clearly so that society can be made aware of the outcomes of the efforts and service providers can compare them against their sector-wide endeavours.

Another aspect to be noted is that cultural change among stakeholders may be gradual and it might take several stages before the new process is completed and consolidated. This involves raising awareness and commitment, including among top management, instilling specific skills in teams, and ultimately institutionalizing the model. In some cases, companies have taken onboard the benefits and cost savings of resolving issues in a responsive manner, redirecting efforts internally instead of escalating administrative debates. This has enhanced their image and led to gains in shareholder interest.

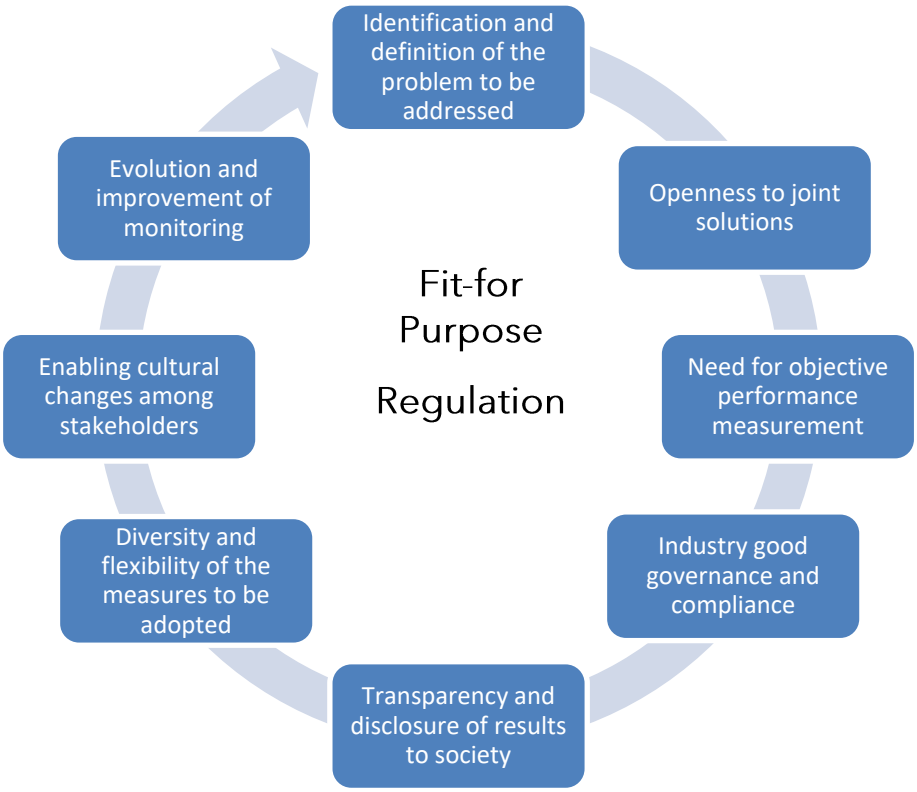
In conclusion, in addition to the continuous monitoring and effective functioning of internal company compliance, there will also be a need to consider the instruments used, periodically review their scope, and identify solutions that keep pace with technological changes and the typical user behaviour in the sector.

2.2 Best practices for regulations to protect consumer rights

A summary of the best practices for regulations to protect consumer rights usually include one or more of the principles below.[19]

- **Identification and definition of the problem to be addressed**: The scope must be well defined, and the expected objectives must be clear to those involved, so that they prioritize efforts and are incentivized to achieve the desired results.
- **Openness to joint solutions**: The solution process should be as open as possible to all involved, so that it responds to the current, actual demands of consumers and society.
- **Need for objective performance measurement**: The focus should be on improving services, but this is not always visible from subjective evaluations. Regulators should have qualitative and quantitative indicators to determine that what is being requested is proportional and necessary for the company to comply with the rules.
- **Industry good governance and compliance**: The agreed general principles and requirements constitute established good practices that should be systematically applied within each company's internal compliance framework as the basis for responsive action, both to ensure the initial success of the proposed implementation and to secure the sustainability of its results.
- **Transparency and public disclosure of results**: The work should be disseminated and communicated in such a way that the public can learn about its results and that providers can also compare the results of efforts in the sector.
- **Diversity and flexibility of the measures to be adopted**: Regulation should be focused on satisfactorily solving identified problems and improving services, with the possibility of making adjustments throughout the processes using responsive tools.
- **Enabling cultural changes among stakeholders**: Several stages may be needed in order to complete and consolidate the new process, and this involves awareness and commitment.
- **Evolution and improvement of monitoring**: Results must be continually studied and discussed, in order to avoid or mitigate the loss of effectiveness of the measures over time.

[19] https://www.itu.int/hub/publication/d-stg-sg01-06-3-2023/


Identification and definition of the problem to be addressed
Openness to joint solutions
Need for objective performance measurement
Industry good governance and compliance
Transparency and disclosure of results to society
Diversity and flexibility of the measures to be adopted
Enabling cultural changes among stakeholders
Evolution and improvement of monitoring
Fit-for Purpose Regulation

Chapter 3 – Digital transformation strategies and relevant issues for consumers

This chapter provides information about policies, frameworks, organizational methods, tools and strategies developed by national regulatory authorities and other organizations that enable digital transformation, and examines the challenges encountered.

The challenges that relate to consumers include online communications and transactions (3.1), unsolicited commercial communications (3.2), online fraud (3.3) and misuse of PII (3.4).

3.1 Online communications and transactions using new and emerging telecommunication/ICTs

Technology is evolving at unprecedented speed and is driving efficiency, security, innovation and engagement in the digital economy and society. New and emerging technologies, such as 5G, IoT, AI, and augmented and virtual reality (AR/VR), are revolutionizing online communications and transactions through real-time connectivity, automation, personalized solutions, transparency, scalable infrastructure and immersive experiences.

The achievement of the digital transformation agenda hinges on the ability of economies to leverage those new and emerging technologies to drive the development of the digital economy and society.[20] In addition, there is a need to build a robust ecosystem that supports this development as ICTs have permeated all aspects of our lives. The dynamism in the ICT sector means that the approaches to consumer protection will continue to evolve.[21]

Increasingly, consumers will participate in shaping the digital economy and society. Their expanded role in the digital ecosystem should be recognized and their participation in the digital economy and society should be facilitated through new and emerging telecommunication/ICTs. In so doing, emerging technologies need to be leveraged to enhance consumers' experiences, implement appropriate measures that enable easy access and use, and acknowledge and adapt to consumers' expectations and preferences.

[20] WTDC-22 Report https://www.itu.int/dms_pub/itu-d/opb/tdc/D-TDC-WTDC-2022-PDF-E.pdf
[21] https://www.itu.int/pub/D-PREF-TRH.1-2020

3.1.1 Strategies to facilitate and enhance consumers' online communications and transactions using new and emerging telecommunications/ICTs and organizational practices

3.1.1.1 Emerging technologies that enhance user experience, online communications and transactions

Innovations in new and emerging technologies are set to bring untold opportunities and benefits for the development and growth of the digital economy and society; from carrying out mundane tasks to providing solutions that enhance the digital transformation. These opportunities transcend all sectors, with solutions focusing on enhancing productivity and job outcomes, the creative process, data analysis, and increasing consumers' trust and confidence in the ICT market, among other benefits.[22] A study of the potential that could be unlocked by AI in Africa shows that the potential benefits in just four sub-Saharan African countries (Ghana, Kenya, Nigeria and South Africa) could reach USD 136 billion by 2030.[23]

The use of immersive technologies has significantly enhanced user experience and has consequently had an impact on user consumption as it combines the real world and virtual experiences. China Mobile has transformed cultural and historical tourism by leveraging 5G and VR technology so that users can immerse themselves in the activities of the ancient cultures.[24]

3.1.1.2 Understanding consumer behaviour in the digital age

The emergence of new technologies can enhance the consumer experience by making a broad variety of products and services more convenient, safe, easily accessible (mobile first) and private, in addition to providing a seamless customer experience and easy payment methods.[25]

New and emerging technologies have already had a significant impact on consumption and consumers derive new values and new experiences as these technologies[26] are leveraged thanks to the integration of online and offline experiences, for example.

These developments are accompanied by challenges[27] related to the potential for harm to users from risks to data protection,[28] data security and PII, AI transparency and ethics, a widening digital divide,[29] and unfair business practices.[30] With regard to the widening of the digital divide, it is notable that vulnerable consumers, such as women, persons with disabilities, older persons, and people living in rural, remote and marginalized areas, are at risk of being left behind.[31] Lacking universal and meaningful connectivity affects their ability to actively participate in the

---

22 ITU-D Document https://www.itu.int/md/D22-SG01-C-0242/ from Access Partnership Limited, UK
23 Ibid
24 ITU-D Document https://www.itu.int/md/D22-SG01.RGQ-C-0231/ from China Mobile Communications Corporation
25 ITU-D Document https://www.itu.int/md/D22-SG01-C-0335/ Report of the workshop on Increasing Consumer Awareness Mechanisms to Promote Informed Consumer Decision: A joint workshop for Question 6/1 and Question 3/2 held in Brasilia from 18-20 June 2024.
26 ITU-D Document https://www.itu.int/md/D22-SG01.RGQ-C-0231/ from China Mobile Communications Corporation
27 ITU-D Document https://www.itu.int/md/D22-SG01-C-0343/ from Cameroon
28 ITU-D Document https://www.itu.int/md/D22-SG01-C-0470/ from Chad
29 ITU-D Document https://www.itu.int/md/D22-SG01-C-0242/ from Access Partnership Limited, UK
30 ITU-D Document https://www.itu.int/md/D22-SG01-C-0325/ from the Republic of the Congo
31 ITU-D Document https://www.itu.int/md/D22-SG01.RGQ-C-0150/ from RIFEN

digital economy and society, a phenomenon that also affects small and medium-size enterprises (SMEs).[32]

In addition, access to factual and trustworthy information has increasingly become a concern,[33] clearly shown by the increased prevalence of misinformation. This is a major issue that has drawn global attention, with some countries, such as China,[34] India, and the United States, and also the European Union, issuing guidelines, advisories, and codes of practice to address deepfakes.[35]

Another issue is the collection of a significant amount of information, including health data and PII, from devices such as security cameras. A study by Kaspersky indicates that IoT devices are increasingly becoming targets for cyberattacks.[36] Incident data document the data protection challenge posed by hackers accessing home video feeds.[37]

3.1.1.3 Strategies to enhance consumer online communications

The increasing complexity of navigating the digital economy and society makes it necessary to empower consumers to make informed purchase and use decisions.[38] In so doing, it is crucial to develop a deeper understanding of consumers' preferences and behaviour in the purchase and use of ICT products and services, and their levels of participation in the digital economy and society. This can be achieved by leveraging behavioural science,[39] as done by Anatel in Brazil and Ofcom in the United Kingdom. In addition, consumers should be empowered to make informed purchase and use decisions by enhancing their access to transparent information and providing decision-making tools,[40] such as comparison tools for tariffs, complaints, and quality of service – a strategy which was adopted by Mexico and Egypt.

In Brazil, in order to address consumer demands for fast, customized and personalized services, telecommunications company Vivo[41] has a number of strategies to enhance engagement with their customers. They include customer journeys that are simpler, clearer and hassle-free, with an omnichannel experience (seamless across platforms) and a customer-centric approach across all digital channels and applications.

In China, a comprehensive system protects consumers' right to know when they are being served by AI, or when a telecommunication/ICT service is using AI. The system focuses on the following: developing a policy to guide the creation of a protection framework for AI consumer rights, with a particular focus on areas such as R&D standards, notification agreements, content labelling and complaint mechanisms; developing standards for AI products and services; upgrading technologies and services to help consumers identify and prevent fraudulent information; and issuing safe AI usage guidelines while promoting AI literacy.[42]

---

32 ITU-D Document https://www.itu.int/md/D22-SG01-C-0242/ from Access Partnership Limited, UK
33 Ibid
34 ITU-D Document https://www.itu.int/md/D22-SG01-C-0505/ from the People's Republic of China
35 ITU-D Document https://www.itu.int/md/D22-SG01.RGQ-C-0150/ from RIFEN
36 ITU-D Document https://www.itu.int/md/D22-SG01-C-0325/ from the Republic of the Congo
37 Ibid
38 ITU-D SG1 Document https://www.itu.int/md/D22-SG01-C-0335/ Report of the workshop on Increasing Consumer Awareness Mechanisms to Promote Informed Consumer Decision: A joint workshop for Question 6/1 and Question 3/2 held in Brasilia from 18-20 June 2024.
39 Ibid
40 Ibid
41 Ibid
42 ITU-D Document https://www.itu.int/md/D22-SG01-C-0505/ from China

3.1.1.4 Strategies to enhance online transactions

Online payments and transactions are very important features of the digital economy and society as they enable users to access ICT products and services. Following the COVID-19 pandemic, the preferred payment method of consumers has shifted to digital,[43] with 98 per cent of surveyed users in Bamako[44] and 77.5 per cent of mobile phone users in mainland China[45]. Secure and seamless online transactions are therefore crucial. Contributions noted that mobile money services, such as M-Pesa, Orange Money and MTN Mobile money, developed faster in markets where there was a combination of high mobile penetration rates and large populations of unbanked consumers.[46]

Consumers have experienced several challenges involving mobile money services, including exposure to fraud and scams, such as the use of AI face-swapping to circumvent facial verification on digital payment applications,[47] and lengthy and bureaucratic processes for correcting errors and resolving complaints.[48] Other challenges include high transaction costs, poor quality of service, a lack of transparency and information regarding complaint processes, and exposure to risks such as the misuse of data,[49] as exemplified by a report from Mali. There is a lack of collaboration among the relevant stakeholders, a lack of regulatory interventions in the handling of consumer complaints and a lack of regulatory oversight in the complaints management systems instituted by mobile money service providers.[50]

Some of the strategies leveraged by the Economic and Monetary Community of Central Africa (CEMAC) to increase consumer confidence and trust in the services include establishing rules that enable consumers to recover funds that were erroneously transferred to an unintended recipient. This required that mobile money transactions, while being immediately credited to the recipient's account, only be made available for use after five minutes, in order to give the sender the opportunity to reverse the transaction.[51]

The contribution from the Republic of the Congo emphasizes the need for regulators and operators to play a greater role and take more responsibility in the fight against mobile money fraud.[52]

To enhance data security, China Telecom's BestPay established a User Protection Centre[53] offering transparent self-service management. AI-driven support improves user engagement, issue detection and experience management, while intelligent risk control products address security concerns. There are also solutions dedicated to older persons.[54]

---

43 ITU-D Document https://www.itu.int/md/D22-SG01-C-0224/ from China Telecommunications Corporation
44 ITU-D Document https://www.itu.int/md/D22-SG01-C-0376/ from Mali
45 ITU-D Document https://www.itu.int/md/D22-SG01-C-0224/ from China Telecommunications Corporation
46 ITU-D Document https://www.itu.int/md/D22-SG01-C-0383/ from the Republic of the Congo
47 ITU-D Document https://www.itu.int/md/D22-SG01-C-0224/ from China Telecommunications Corporation
48 ITU-D Document https://www.itu.int/md/D22-SG01-C-0383/ from the Republic of the Congo
49 ITU-D Document https://www.itu.int/md/D22-SG01-C-0376/ from Mali
50 Ibid
51 ITU-D Document https://www.itu.int/md/D22-SG01-C-0383/ from the Republic of the Congo
52 ITU-D Document https://www.itu.int/md/D22-SG01-C-0475/ from the Republic of the Congo
53 ITU-D Document https://www.itu.int/md/D22-SG01-C-0224/ from China Telecommunications Corporation
54 Ibid

3.1.2 Best practices to enable digital transformation

To drive digital transformation with a consumer-focused approach, regulators should encourage organizations to adopt the following practices:

- **Implement consumer-centric policies and guidelines:** Develop frameworks that prioritize users' needs. Ensure regulations support digital innovation while protecting consumers.
- **Leverage emerging technologies**: Enhance digital products and services through new and emerging technologies, such as AI, for fraud detection and cybersecurity. Adopt an omnichannel approach to improve consumer engagement.
- **Educate and empower consumers:** Design programmes using both traditional and emerging technologies to inform users about digital tools and evolving consumer issues.
- **Address emerging consumer concerns:** Establish mechanisms to handle ethical, environmental, health, PII and data protection challenges faced by consumers.
- **Strengthen internal consumer protection measures:** Implement internal control systems and risk prevention frameworks to safeguard consumers.
- **Foster a consumer-centric culture**: Promote innovation and responsiveness to consumer needs at all levels of the organization.
- **Build a transparent and accountable digital ecosystem:** Develop a supportive infrastructure that ensures responsible digital transformation while maintaining trust and transparency.

3.2 Unsolicited commercial communications

Unsolicited commercial communications, or spam, are unwanted and often invasive digital messages sent in bulk via text, calls, emails or social media.

In telecommunications, the issue of unsolicited commercial communications has been a problem for consumers around the world, with several countries adopting laws or regulations to control, regulate, or enforce responsible text marketing practices and apply penalties for irresponsible practices.

In Nigeria,[55] MNOs have adopted various telemarketing strategies to disseminate information to their subscribers about the services and offerings available on their network. These have caused an upsurge in the number of complaints from consumers about unsolicited telemarketing messages and robocalls. As a result, NCC issued a regulatory instrument which required MNOs operating in Nigeria to:

1. Create a database of consumers' preferences regarding the Do-Not-Disturb (DND) service.
2. Dedicate the short code '2442' for subscribers to opt into the database at no charge as a means of restricting unsolicited telemarketing messages from one or more of the following categories: news alerts, religious messages, sports, education, health and tourism.
3. Create awareness of the availability of the DND service on the various networks among consumers.
4. Ensure that only authorized, network-generated SMSs are sent to consumers between the hours of 8 a.m. and 8 p.m.
5. Impose administrative fines if operators fail to comply with the regulatory instrument, in order to serve as a deterrent to non-compliance.

[55] ITU-D Document https://www.itu.int/md/D22-SG01-C-0032/ from Nigeria

6. Exempt financial transaction alerts and election-related messages from the DND service to prevent fraud and ensure information flow in the election. Exemptions also apply in public emergencies and safety situations.

In this regard, China[56] prioritizes consumer rights by improving the consumption environment, balancing development with regulation and strengthening legal protections. It continuously updates laws and standards, emphasizing digital rights and safeguarding vulnerable consumers.

Rwanda[57] has implemented several controls and regulations to limit unsolicited commercial communications while promoting responsible and consensual marketing practices. The regulation requires commercial electronic messages to include accurate information about the person who authorized the sending of the message and a functional unsubscribe option to enable the recipient to instruct the sender to cease all future communications. It also prohibits address-harvesting software and the use of harvested address lists for sending unsolicited commercial electronic messages, and, more generally, discourages people from using ICTs inappropriately.

The Telecommunications Regulatory Commission of Sri Lanka (TRCSL)[58] issued an operator self-governance policy on promotional messages which elaborates the procedures to be adopted by operators on promotional messages mediated by operators and promotional messages generated by external parties.

For promotional messages generated by external parties, the following procedures were adopted:

1. Operator shall register Ports/Clients that: (i) are authorized to generate Promotional Messages; and (ii) warrant to the Operator that all messages transmitted would be with the consent of consumers registered with the said client.
2. Only registered Ports/Clients should be able generate Promotional Messages to their respective registered customers. Promotional Messages generated by unregistered Ports/Clients will be blocked.
3. Operator will register, investigate and take action on all customer complaints received pertaining to unsolicited messaging via SMS Ports/Clients, or via standard mobile numbers. Such action could include the disconnection of port or permanent blocking of a number mask or mobile number.
4. Operator will publish information on free of charge methods of blocking promotional messages generated by a particular port number mask in its website and other customer information channels.

While for Promotional Messages Mediated by Operator (within the control of Operator)

1. Each promotional message shall carry an opt-out option to enable the customers to conveniently discontinue receipt of promotional messages from the relevant Service Provider/Port/Number Mask.
2. Each Promotional Message shall be generated under a number mask to uniquely identify the originator of the promotional message.
3. Each promotional message shall contain an Opt-out option to stop receipt of such information.
4. Opt-out or SMS block facility shall be provided free of charge.

---

[56] ITU-D Document https://www.itu.int/md/D22-SG01.RGQ-C-0069/ from Beihang University
[57] ITU-D Document https://www.itu.int/md/D22-SG01-C-0155/ from Rwanda
[58] ITU-D Document https://www.itu.int/md/D22-SG01-C-0125/ from Sri Lanka

5. Opt-out or SMS block methods for Operator Promotional Massages shall be published on Operator's website and communicated via multiple customer information mediums.

Despite the implementation of the above self-governance policy guidelines, there were increasing complaints from consumers regarding excessive, intrusive and non-compliant promotional messages specifically in relation to unsolicited promotional messages and telemarketing practices. In this context TRCSL prepared a code of practice for telecommunication operators to close loop-holes in previous guidelines and enhance consumer protection.[59]

In Brazil,[60] different measures were adopted to tackle the problem of abusive calls, such as encouraging the adoption of good practices, blocking the ability to originate calls if certain calls or efficiency limits are exceeded and improving the quality of information for consumers. Anatel established initiatives to empower users in the fight against abusive telemarketing, debt collection, and similar calls. These initiatives aimed to combat specific aspects of the problem, such as the misuse of numbers, mass calling, and violating the rights of users. The initiatives are detailed below:

1. The Do Not Call Registry, which is made up of consumers who have opted out of receiving calls offering telecommunication products and services, and, in parallel, a code of conduct for standardize the treatment of calls.
2. The requirement that telemarketing companies and entities responsible for large volumes of calls (above 10 000 daily calls) use the 0303 prefix, regardless of the reason for the call, so that consumers could identify the caller and decide whether to answer.
3. A precautionary decision based on three pillars of action: maintaining a ceiling on the volume of calls per access (source number); encouraging user efficiency when using telecommunications networks; and creating rules that will make the origin of calls more transparent. The decision considers that the use of technological solutions for carrying out mass calls in a volume greater than the normal human capacity for dialling, answering and communicating would allow, and in such a way that the calls disconnect within three seconds if completed or not (known as short calls), constitute a misuse of numbering resources and an inappropriate use of telecommunications services. Network operators identify the source and block, for a period of 15 days, the ability to originate calls from the accesses of the fixed switched telephone service (landlines) and the personal mobile service (cell phones) of legal entities that:
    a. Generate at least 100 000 short calls per access code in one day; or,
    b. Generate at least 100 000 calls and in which the total number of short calls represents a proportion equal to or greater than 85 per cent of the total calls.
4. This decision also required that telecommunications service providers that use numbering resources work together to provide an Internet search tool that can be used to identify the holder of the access codes of fixed and mobile phones held by legal entities. The tool in question can be accessed through the Internet portal www.qualempresameligou.com.br/ .
5. Implementation of the Verify Origin (formally known as STIR/SHAKEN) call authentication and identification protocol which lets consumers see the caller ID number; the caller's identification, name and logo; the reason for the call; and a digital stamp that attests to the caller's origin (rich call data). With this information, consumers can identify companies' calls and decide if they are interested in answering them.
6. Coordination with the Brazilian National Data Protection Authority with the aim of planning structural measures against data brokers: companies that specialize in compiling public information shared by other companies and are a component of the teleservices chain

[59] ITU-D Document https://www.itu.int/md/D22-SG01-C-0492/ from Sri Lanka
[60] ITU-D Document https://www.itu.int/md/D22-SG01-C-0453/ from Brazil

whose activities greatly influence the volume of calls received by the public. Dozens of legal proceedings are under way against telecommunications companies, teleservices and their contractors.

In Australia,[61] the regulator conducts ongoing enforcement and compliance activities to combat telecommunications scams and takes actions against providers for compliance failures. The regulator also issues consumer alerts about government agency impersonation and remote access scams. Several government and industry-led measures to combat telecommunications scams have also generated positive results. The initiatives are listed below:

1. Specifying 7226 (SCAM) as a shared special community service number (for voluntary use by telecommunications providers, to provide a quick and easy way for their customers to directly report scams).
2. Preventing Freephone, local rate, and premium rate numbers from being used for outbound calls (to stop scammers using these numbers to gain consumers' trust during scam calls).
3. Giving the regulator the power to withdraw a number associated with scamming or other fraudulent activity.
4. Registering the Reducing Scam Calls and Scam SMS Code which includes requiring telecommunications providers to:
    - Identify, trace and block scam calls and scam texts.
    - Publish information to assist their customers to proactively manage and report scam calls and texts.
5. Mandating stronger identity verification processes before mobile numbers can be transferred between providers via the Telecommunications Industry Standard 2020 to prevent scammers hijacking mobile phone numbers to steal from people's financial accounts.
6. Mandating stronger identity verification processes for high-risk transactions (including SIM swap and account change requests) via the Telecommunications Service Provider Determination 2022 to prevent unauthorized access by malicious actors to people's telecommunication services and personal information.
7. Having telecommunications service providers use scam filters to identify and block malicious SMS with suspicious links/ telephone numbers before they reach customers' mobile phones.
8. Targeting call-back scams with the Call Stop initiative. In partnership with a telecommunications provider, the initiative targets call back scams, where customers receive an email or SMS claiming issues with their bank account. The communication requests customers call back the bank on the number provided – where they reach a scammer impersonating the bank. Here, scammers trick the consumer into providing access to their account or transferring money into an account controlled by the scammer. Until the identified scam number is blocked, the Call Stop initiative prevents customers who call the identified scam number from reaching the fraudster, instead forwarding the call to an automated message that warns customers they are the target of a scam.

3.2.1 Best practices on unsolicited commercial communications

1. The digital transformation needs consumers to feel safe and protected when opting to use a new service, and therefore countries are advised to have regulatory frameworks for dealing with unsolicited commercial communications, along with penalties and enforcement mechanisms that address wrongdoing and hold parties accountable when necessary.

[61] ITU-D Document https://www.itu.int/md/D22-SG01-C-0212 from Australia

2. Countries should establish a legal and regulatory framework that supports the development of the digital world by implementing regulations that protect against the misuse of consumers' PII, and increasing the transparency of how consumer information is acquired and used in communications.
3. To address the evolving needs of consumer protection in the digital era, countries are encouraged to continuously adjust and improve relevant policies and regulations by actively promoting the digital transformation within the framework of traditional consumer protection laws.
4. Markets should respect that unsolicited commercial communications are generally considered disruptive and unwelcome. Working with all stakeholders on ethical and effective marketing strategies can mitigate the effects of this challenge.
5. Given the extreme complexity of unsolicited commercial communication, a variety of complementary preventive measures should be adopted.
6. Co-regulation or a holistic approach should be adopted where appropriate to encompass industry and government initiatives in aid of public policy objectives, alongside continued consumer awareness campaigns to empower consumers.
7. International cooperation with other countries and international regulators to strengthen strategic engagement in the global fight against scams, unsolicited telemarketing and spam should be facilitated as it will help share spam information, target priority scams and raise awareness.

Some ethical and effective strategies for handling unsolicited commercial communications include the following:

1. Consumer education and empowerment, in addition to collaboration among various stakeholders are crucial to address emerging challenges, enhance transparency and foster building trust in the digital economy. This approach is key to effectively safeguarding consumers in a constantly evolving digital landscape.
2. Effective unsubscribe and opt-out/opt-in mechanisms that enable customers to prevent further messages from the respective service provider or specific application.
3. Marketers or business entities should obtain explicit written, not verbal, consent to add anyone to their subscription list, before sending promotional messages with the intent to sell, upsell or advertise a product, business or service.
4. Even if a consumer provides their telephone number and has a long-standing relationship with the company, written consent should be required before sending commercial communications.
5. Permission-based marketing involves obtaining consent from customers before sending commercial communications. Implement a double opt-in process for subscriptions, in which users confirm their interest in receiving messages.
6. Make sure that consumers are willing to receive transactional text messages that keep them up to date on important information or help them perform an action that does not result in a sale.
7. Marketers and business entities shall provide important information, such as their identity, messaging frequency, an opt-out method and the applicable charges, in the first text message to the consumer before confirming opt-in.
8. Include clear and compliant calls to action at the end of each message, which include the campaign's purpose, frequency, terms and conditions, privacy policy, information about the message, and data rates.
9. Impose penalties for breaking SMS marketing laws and rules.
10. Ensure telemarketing companies use a specific number prefix for unsolicited commercial communications.
11. Establish a Do Not Disturb Register or Do Not Call Registry that enables people and businesses to opt out of unsolicited marketing or sales calls and other forms of communication.

12. Telecommunications service providers should be encouraged to use scam filters to identify and block malicious SMS and calls with suspicious links or telephone numbers before they reach customers.
13. Telecommunications providers must monitor and identify those responsible for high volumes of calls and enforce their compliance with the rules under the regulator's supervision.

3.3 Online fraud

3.3.1 The overall trend of online fraud

The rapid development of cyber and information technology has led to an explosion of online fraud. From the relatively simple text message and phone scams in its early days, online fraud has become a sophisticated industry that uses advanced technology and innovative tactics. In the following, three of the main trends observed today are outlined.

First, it can be seen that cyberspace, characterized by openness, diversity, virtual identities, and convenient interactions, provides an enabling environment for certain fraudulent activities. Fraudsters may use personal information to falsely gain consumers' trust. This makes it easier to bypass the security mechanisms put in place by payment institutions, telecoms operators and other service providers. In this way unwary victims can be defrauded, causing not only financial losses but also mental and emotional distress etc. For instance:

- In Uganda, there are 24.1 million active e-money users, with a national penetration rate of 56 per cent, all of whom are potential victims of online fraud.
- In the Republic of Korea,[62] criminals rely on ID theft to obtain mobile phones for illicit activities, resulting in between 200 and 300 such phones being used for various frauds in 2022, according to the Korean police.
- In Australia, consumer losses due to scams reached a record AUD 3.1 billion in 2022, significantly impacting both victims and the broader economy.

According to the Truecaller Global Scam and Spam Report (2022), Brazil has been in the worst position for the past four years, with 32.9 spam calls per user per month; that is almost double that of the next-worst performer, Peru, with 18.02 calls per user per month.[63] Monetary loss from scams and ID theft has a significant impact on victims and the broader economy.[64]

Second, each iteration in the ongoing renewal of emerging technologies brings with it the risk of exploitation by online fraudsters who monitor such developments closely. Online fraud can relate to and enable other activities, such as infringement of PII, and operate in synergy with an entire chain of black and grey operators, with online fraud at the centre.

Thus, fraudulent AI-generated content, including deep fake videos, is used to deceive individuals in targeted scams.[65] For example, in China, where digital payment platforms rely heavily on facial verification for account log-in, transaction verification and account unfreezing, fraudsters have switched to technologies such as AI-powered face-swapping, causing significant losses to consumers.[66] In India, scammers impersonate courier services or law enforcement and use

[62] ITU-D Document https://www.itu.int/md/D22-SG01-C-0152 from the Republic of Korea
[63] ITU-D Document https://www.itu.int/md/D22-SG01-C-0145/ from Brazil
[64] ITU-D Document https://www.itu.int/md/D22-SG01-C-0212/ from Australia
[65] ITU-D Document https://www.itu.int/md/D22-SG01-C-0356/ from RIFEN
[66] ITU-D Document https://www.itu.int/md/D22-SG01-C-0224/ from China

leaked personal information to trick victims. One-time password-based scams have also caused significant financial losses due to the rise in digital payments.[67]

Third, certain types of people are particularly vulnerable to online fraud. In China, the National Research Report on Internet Use by Minors (2021) shows that the proportion of underage Internet users who have been affected by online scams has increased.[68] In addition, 20 per cent of underage Internet users have no concept of how to counteract online fraud, privacy breaches, harassment, etc., and very young children tend to be particularly unaware.[69]

Dealing with these manifestations of online fraud stretches the resources of many countries. As mentioned in the contribution from Liberia, only 25 countries of the 54 African countries have laws related to online consumer rights and electronic transactions, and 4 more are currently drafting legislation.[70] In many cases the existing laws are out of date and badly suited to combating novel forms of consumer online fraud. For example, in Uganda, laws on electronic transactions and computer crimes were enacted in 2011, and are no longer up to the task of ensuring the protection of online consumer rights.[71] Similarly, in South Africa, the regulation of false advertising is still based on a Consumer Protection Act dating back to 2008.[72]

3.3.2 Innovative measures for dealing with online fraud

3.3.2.1 Improving relevant policy and legislation

Many countries are upgrading their legislation to protect the rights and interests of consumers.

India has amended its laws relating to electronic transactions by incorporating information technology crimes into the IT Act 2000 and by introducing the word "electronic" into the Indian Penal Code, explicitly including electronic records and documents in the same category as physical records and documents.[73]

In 2023, the Government of **India** released a draft of proposed Guidelines for Prevention and Regulation of Dark Patterns to curb the menace of dark patterns that harm consumers online. Dark patterns are defined as "*any practices or deceptive design patterns using UI/UX (user interface/user experience) interactions on any platform; designed to mislead or trick users to do something they originally did not intend or want to do; by subverting or impairing the consumer autonomy, decision making or choice; amounting to misleading advertisement or unfair trade practice or violation of consumer rights*".[74]

In **South Africa**, the Consumer Protection Act explicitly regulates false and misleading advertising to protect consumers from unscrupulous advertisers.[75]

Uganda's online crime legislation, has made online consumer fraud a punishable offence.[76]

---

67 ITU-D Document https://www.itu.int/md/D22-SG01-C-0302/ from India
68 ITU-D Document https://www.itu.int/md/D22-SG01.RGQ-C-0222/ from China Mobile Communications Corporation
69 Ibid
70 ITU-D Document https://www.itu.int/md/D22-SG01.RGQ-C-0004/ from Liberia
71 Ibid
72 Ibid
73 Ibid
74 ITU-D Document https://www.itu.int/md/D22-SG01-C-0196 from ITU-APT Foundation, India
75 ITU-D Document https://www.itu.int/md/D22-SG01.RGQ-C-0004/ from Liberia
76 Ibid

In **China**, the Supreme People's Court, the Supreme People's Procuratorate, and the Ministry of Public Security in 2016 jointly issued opinions regarding the application of law in the handling of telecommunications network fraud and other criminal cases. In order to further punish online fraud and to implement a full-chain and all-round crackdown on such activities, in December 2022, China officially implemented the Combating Telecom and Online Fraud Law, setting out the responsibilities of local governments, industry regulatory departments, and enterprises, as well as the measures they must take, for prevention and governance.[77]

In **Brazil**, Anatel's strategic plan for 2023-2027 has taken strategic action to prevent fraud and scams in the digital ecosystem, promoting cybersecurity awareness and enhancing the digital security of citizens.[78] Other initiatives combat specific aspects of the problem, such as misuse of numbers, mass calling, and infringements of the rights of users.[79]

In **Australia,** the ACMA has introduced several new rules to disrupt scammer activity: (a) amending the Telecommunications Numbering Plan 2015 to support several scam disruption initiatives; (b) registering the Reducing Scam Calls and Scam SMS Code in July 2022, requiring telecommunications providers to identify, trace and block scam calls and scam texts, and to publish information to assist customers to manage and report scam calls; (c) mandating stronger identity verification processes before mobile numbers can be transferred between providers via the Telecommunications (Mobile Number Reporting Additional Identify Verification) Industry Standard 2020; and (d) mandating stronger identity verification processes for high-risk transactions via the Telecommunications Service Provider (Customer Identity Authentication) Determination 2022.[80]

3.3.2.2 Improving monitoring and enforcement mechanisms

This is being done in three ways. First, many countries establish platforms for consumer complaints. In **Nigeria**, the NCC has set up a toll-free multichannel platform for receiving complaints submitted in writing, on a consumer portal, by e-mail, via Facebook, Twitter and Instagram accounts and so on, to build a bridge between consumers and the Commission and ensure that consumer complaints are effectively resolved.[81] BTK, **Turkey**'s national regulator for the electronic communications and postal sector, requires service providers to establish a system to resolve consumer complaints in a manner that is transparent, rapid, and straightforward, with procedures and principles to resolve complaints and requests.[82]

Second, advisory bodies have been established to provide recommendations on regulatory matters. In **Côte d'Ivoire**, the Consumer Council established by ARTCI is tasked with proposing opinions, draft decisions, etc. on regulatory matters falling under the responsibility of ARTCI: protecting privacy and confidentiality, and preventing and combating online crime, in order to protect and safeguard the legitimate rights and interests of consumers by allowing them to participate personally in the regulatory authority's decision-making process.[83]

Third, mechanisms to monitor and enforce compliance are being strengthened, and a dynamic regulatory model is being promoted that combines external discipline with internal incentives.

---

77 ITU-D Document https://www.itu.int/md/D22-SG01.RGQ-C-0069/ from Beihang University
78 ITU-D Document https://www.itu.int/md/D22-SG01.RGQ-C-0251/ from Brazil
79 ITU-D Document https://www.itu.int/md/D22-SG01-C-0145/ from Brazil
80 ITU-D Document https://www.itu.int/md/D22-SG01-C-0212/ from Australia
81 ITU-D Document https://www.itu.int/md/D22-SG01.RGQ-C-0020/ from Nigeria
82 ITU-D Document https://www.itu.int/md/D22-SG01.RGQ-C-0089/ from Türkiye
83 ITU-D Document https://www.itu.int/md/D22-SG01.RGQ-C-0042/ from Côte d'Ivoire

In **Brazil,** Anatel has adopted an enforcement mechanism that imposes fines and other sanctions for fraud and other violations detected in telecommunications services. Anatel proposed the theory of responsive regulation, which provides flexible and varied compliance regulation of telecommunications service providers based on specific circumstances to ensure proper and regulated operation, prevent online fraud, and meet the needs of consumers.[84]

In **Australia,** in April-June 2023 the ACMA took action against three providers after their compliance failures allowed SMS to be sent using text-based sender IDs without sufficient checks to ensure they were not being used by scammers.[85]

3.3.2.3 Cooperation with platforms and stakeholders

Given the complexity of online scams, many countries are enhancing their cooperation with stakeholders such as platforms to achieve more effective scam prevention, disruption and resolution. Several approaches are being used.

The first is to strengthen information-sharing between government and IT industries.

The **Uganda** Communications Commission focuses on mobile payment fraud and works with several key stakeholders, including the Central Bank, the National Identity Registration Authority, the Association of Financial Technology Service Providers, the Communications Computer Emergency Response Team and consumer advocacy organizations, to facilitate the implementation of regulatory initiatives for SIM card registration and verification, to build the capacity of stakeholders, and to create a safe and secure environment in the area of mobile payments to prevent and combat fraud related to mobile payments.[86]

In **Egypt**, a service called My Lines allows individuals to use their national ID to find out directly how many mobile lines are registered against their names across all mobile operators working in the country. This protects the privacy of subscribers and helps reduce fraudulent operations.[87]

Australia has strengthened cooperation with stakeholders by establishing the National Anti-Scam Centre in July 2023 to bring together law enforcement, telecommunication providers, digital platforms and others to share scam information, target priority scams and raise awareness.[88]

Another approach is to encourage companies to innovate so as to improve mechanisms to combat online fraud.

In **Australia**, larger telecommunications providers use scam filtering. Telstra, the largest telecommunications provider in the country, operates an SMS scam filter to identify and block malicious messages with suspicious links or telephone numbers before they reach a customer's mobile phone. This is done by scanning the content of an SMS for suspicious patterns and characteristics. Experts review suspicious messages to identify scams – while the details of the recipient remain hidden. Also, the second largest telecommunications provider in Australia, Optus, announced in July 2023 that it had partnered with the Australian Financial Crimes Exchange and banking members. It introduced the Call Stop initiative to prevent Optus

---

84 ITU-D Document https://www.itu.int/md/D22-SG01.RGQ-C-0039/ from Brazil
85 ITU-D Document https://www.itu.int/md/D22-SG01-C-0212/ from Australia. ACMA reports on these compliance failures can be viewed at https://www.acma.gov.au/publications, under the 'Scams' category.
86 ITU-D Document https://www.itu.int/md/D22-SG01.RGQ-C-0046/ from Uganda
87 ITU-D Document https://www.itu.int/md/D22-SG01.RGQ-C-0190/ from Egypt
88 ITU-D SG1 Document https://www.itu.int/md/D22-SG01-C-0212/ from Australia

customers who call the identified scam number from reaching the fraudster until the number is blocked and instead forwards the call to an automated message to warn customers of the scam: *"The number you have called has been reported as being used for scam activities. For more information, please visit* optus.com.au/CallStop*"*. This alerts people that they are being targeted by a scammer.[89]

The **Chinese** company BestPay has established internal management mechanisms for customer service, customer education guarantee systems, comprehensive internal control systems, and full-process risk management systems to comply with the organization's social responsibility regarding the protection of consumer rights and interests, including confidentiality. BestPay uses multiple online and offline channels to educate consumers about security, which includes basic and enhanced awareness and skills in protecting their personal information and data. Online channels include messages, official self-media platforms and personalized push information.[90]

The third approach is to strengthen the obligations and legal responsibilities of companies in combating online fraud.

In the Republic of the Congo, regulators hold the online platforms such as social networks, marketplaces and search engines accountable in matters of advertising and protection of the consumer against dangerous products, counterfeits and fraud.[91]

In Australia, the ACMA conducts ongoing compliance activity to combat scams and audits telecommunications providers that send bulk text messages, revealing that in some cases, scammers used vulnerabilities created by non-compliance to send high-profile SMS scams to Australians.[92]

3.3.2.4 Enhancing consumers' digital capacity and awareness

Increased consumers' awareness of security issues and their digital capacity to deal with them can help prevent online fraud and other malicious activities. For this reason, several countries attach great importance to consumer education and guidance. ITU Datahub reveals that **80.7 per cent of ICT regulators** have consumer education programmes among their responsibilities. In addition, countries have put in place a variety of measures including publicity campaigns and digital skills counselling for special groups such as women, children and older persons, as well as increased publicity and guidance on information applications, online payments, risk screening and other relevant knowledge, to raise consumers' awareness of preventive measures.

South Africa has set up a domain name authority, the African Domain Authority (ZADNA), to provide courses and training for consumers, including women and persons with disabilities, regarding best practices for protecting their domain names with strong passwords, multi-factor authentication, etc., and to better identify security risks in cyberinfrastructure and thus prevent inappropriate behaviour such as online fraud.[93]

Côte d'Ivoire has established a chain of permanent community centres with the aim of educating consumers about their rights. Through regular training on developments in digital technology and consumer rights pertaining to the use of ICT goods and services, it contributes to narrowing

[89] ITU-D Document https://www.itu.int/md/D22-SG01-C-0212/ from Australia
[90] ITU-D Document https://www.itu.int/md/D22-SG01-C-0224/ from China Telecommunications Corporation
[91] ITU-D Document https://www.itu.int/md/D22-SG01.RGQ-C-0147/ from the Republic of the Congo
[92] ITU-D Document https://www.itu.int/md/D22-SG01-C-0212/ from Australia
[93] ITU-D Document https://www.itu.int/md/D22-SG01.RGQ-C-0073/ from South Africa

the digital divide and putting consumers in a position to identify and appropriately deal with risks such as online fraud.[94]

China has established a long-term social support system specifically for older consumers, providing advice and targeted explanations for common tasks that older persons perform online by organizing public interest classroom activities on fraud prevention. The National Anti-Fraud Centre prepared and produced the 2023 edition of an educational manual on the prevention of fraud on telecommunication networks .[95]

The manual sets out the current situation of telecommunication network fraud. It describes 10 common types of high-incidence online fraud in detail, analyses typical cases, exposes fraudulent practices, and provides anti-fraud tips for vulnerable groups. Focused on prevention, the manual encourages the general public to jointly build a "firewall" against online fraud. It is an effective contribution to enhancing fraud awareness among vast numbers of consumers and their ability to recognize and prevent fraud.

Mexico holds workshops on indigenous language translation to promote the use of indigenous languages in the production of content, to raise awareness among indigenous people about their rights as users, potential threats, and how to protect their rights and interests.[96]

Finally, **BestPay** has launched "Security Classroom", a personal information security education column on WeChat public accounts and mobile apps. It uses long-form visuals, animations and short videos on financial security covering a wide range of topics such as financial basics, cybersecurity, privacy, combating money laundering and cyber fraud, protection of consumer rights.[97]

3.3.2.5 International collaboration

International collaboration plays an important role in the fight against fraud. In **China,** the Combating Telecom and Online Fraud Law of the People's Republic of China specifically calls for effective cooperation mechanisms with relevant countries, regions and international organizations to be established. International cooperation in law enforcement and other areas enhances information sharing, investigations, the collection of evidence, detection and arrest of fraudsters, and recovery of stolen goods and losses, effectively combating and curbing cross-border online fraud.

In **Australia**, the ACMA undertakes international cooperation with other nations and international regulators to strengthen strategic engagement in the global fight against scams, unsolicited telemarketing and spam. This cooperation is facilitated by a recently renewed memorandum of understanding that provides for further engagement and information-sharing between agencies.[98]

---

94 ITU-D Document https://www.itu.int/md/D22-SG01.RGQ-C-0056/ from Côte d'Ivoire
95 ITU-D Document https://www.itu.int/md/D22-SG01.RGQ-C-0068/ from China Mobile Communications Corporation
96 ITU-D Document https://www.itu.int/md/D22-SG01.RGQ-C-0101/ from Mexico
97 ITU-D Document https://www.itu.int/md/D22-SG01-C-0224/ from China Telecommunications Corporation
98 ITU-D Document https://www.itu.int/md/D22-SG01-C-0212/ from Australia

3.3.3 Best practices in combating online fraud

Based on the legislation and practical experiences of various countries in combating online fraud, we have summarized the following widely recognized best practices.

1. **Consider regular updates to telecommunications/ICT policies and regulations to address online fraud**: Regularly amend and update telecommunications/ICT policies and regulations to address the evolving nature of online fraud in consultation with all relevant stakeholders.
2. **Establish clear regulatory frameworks**: Introduce specific provisions to address deceptive practices and fraud and ensure the protection of consumer rights pertaining to telecommunications/ICT.
3. **Effective enforcement mechanisms**: Implement robust regulatory oversight with penalties for violations, where appropriate, and ensure compliance.
4. **Promote consumer complaint mechanisms**: Make available complaint-handling mechanisms that provide consumers with expeditious, fair, transparent, inexpensive, accessible, speedy and effective dispute resolution free of any unnecessary cost or burden.
5. **Encourage public-private collaboration**: Foster partnerships between government agencies and private platforms to share information and enhance fraud prevention, and engage platforms to be responsible for preventing online fraud and protecting consumers.
6. **Increase digital literacy and consumer awareness**: Implement comprehensive educational campaigns to raise awareness of online fraud, targeting all demographic groups, particularly vulnerable populations.
7. **Encourage strong verification processes for online transactions and mobile services**: Encourage verification processes for online transactions and mobile services to help prevent fraudulent activities against consumers.
8. **Foster international collaboration**: Strengthen cross-border collaboration across governments, regulators and other stakeholders to share best practices to combat online fraud.
9. **Support technological innovation for fraud prevention**: Encourage the development and use of technology solutions to detect, prevent and mitigate online fraud.
10. **Implement continuous risk monitoring**: Regularly assess and update fraud prevention strategies to stay ahead of emerging cyberthreats and vulnerabilities.

3.4 Misuse of personally identifiable information

3.4.1 Background

In today's society, the volume of information distributed in the economy is soaring as transactions increasingly dispense with face-to-face contact, such as online shopping and delivery apps. This has been made possible because digital technology, networks, AI and cloud storage have made it much easier to collect, maintain and analyse information about individuals. As more and more personal information is used for both public and private purposes, the risk of misuse or abuse of personal information, including theft, has increased as well.

Personally identifiable information (PII) is any information that can be used to distinguish or trace an individual's identity, such as name, date and place of birth, biometric records (e.g. retina scan, voice signature, facial geometry, etc.), and any other information that is linked or linkable to an individual, such as medical, educational, financial and employment information. Examples of PII range from an individual's name or email address to financial, medical and telecommunication records, geographical indicators, religious affiliation, legal records, etc. Unauthorized access to PII or its use or disclosure can cause serious harm both to individuals – by contributing to

identity theft, blackmail or embarrassment – and the organization – by undermining public trust or creating legal liability.

Policy-makers face the dual challenge of how best to enable the use of PII to spur innovative services and enhance consumer welfare in the digital economy while establishing appropriate administrative, technical and physical safeguards to ensure the security and confidentiality of records and protect against any potential harm or inconvenience to individuals whose PII is being collected.

The protection of PII commonly entails protecting the confidentiality, integrity and availability of that information. Most security controls used for other data types also apply to protecting PII. Nevertheless, there are several privacy-specific safeguards for PII, such as anonymization, minimization of PII collection, and de-identification. This is why PII needs to be treated differently from other types of data; it has to be collected, maintained and disseminated in accordance with rigorous privacy principles and appropriate personal information protection regulations. Many countries have privacy laws or regulations in place to protect PII, and international guidelines, such as the OECD Privacy Guidelines, are beneficial[99] and have become the reference for privacy laws and related policies in many countries.

3.4.2 PII policy in the Republic of Korea

Social concern about the harmful effects of misuse of PII is on the rise in the Republic of Korea. According to a 2022 white paper by the Personal Information Protection Commission, the national data protection agency, official reports of privacy infringements totalled 210 767 cases in 2022, a rise of 18.8 per cent from the previous year; the number of reports (consultations included) had doubled since 2017.

The most commonly reported forms of PII misuse or abuse of PII are: 1) identity theft via mobile phone,[100] 2) abuse of personal online shopping account[101] and 3) theft of personal customs clearance code or customs ID number.[102]

Privacy protection is the subject of the Personal Information Protection Act (PIPA). Article 3 of PIPA offers eight principles of personal information protection, mandating that data controllers process PII in a manner that minimizes privacy infringement and follows rigorous anonymization procedures.[103]

In response to the rising incidence of identity theft and other privacy infringements, regulators introduced the PII Anonymization Guidelines in August 2020. The guidelines have not had the desired impact on the behaviour of data controllers, and other efforts have been made to promote the anonymization of personal information, such as the Policy to Promote the Use of Anonymized PII announced by the fourth Industrial Revolution Commission of the President's Office in July 2021.

---

99 OECD, Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, 1980.

100 Identity theft via mobile phone: mobile phones are obtained by using stolen personal identification and used for criminal activities. According to the police, there were 200 300 of such phones in 2022, and used for various types of phone frauds.

101 Abuse of personal online shopping account: the information of personal shopping accounts is hacked by credential stuffing attacks, and the PII are then illegally sold on the dark web for use in cyberattacks.

102 Theft of personal customs clearance code: stolen codes are used to avoid taxes or circumvent import regulations, or for smuggling and other illegal imports.

103 See Article 3 of the Principles for Protecting Personal Information here.

PIPA amended the existing PII Anonymization Guidelines on 28 April 2022, in an attempt to clarify the rules and provide greater protection and trust in the use of PII in the economy. The improved guidelines offer detailed step-by-step procedures for the treatment (de-identification) of personal information, processing of personal information and anonymization level, as well as offer various anonymization case examples and FAQs for data controllers. The improved guidelines describe a six-step process for anonymizing PII, summarized below.

Amended PII Anonymization Guidelines (April 2022)

Step 1: Pre-treatment stage: check whether documents and collected data are in conformity with the law, obtain consent from data subjects on the use of PII.

Step 2: Purpose of collection: check whether collected data meets the requirements under the law, prepare legal documentation for the anonymization of PII.

Step 3: Risk management: check whether collected data conforms to the guidelines of risk assessment, refer to the PII classification checklist and standards guideline.

Step 4: Rigorous anonymization process: check whether the process of anonymization was properly applied for each category of PII collected, and whether it complies with the legal guidelines and procedures.

Step 5: Appropriateness of anonymization results: check whether anonymization was fully realized, apply additional levels of anonymization if necessary, and prepare for documentation of anonymization to meet legal obligations.

Step 6: Check for realization of anonymization objectives: confirm whether the anonymization of information was achieved in accordance with stated objectives, obtain documentation of proof of anonymization of PII for submission.

3.4.3 Facilitating consumer protection through information in Mexico[104]

The Federal Telecommunications Institute of Mexico has developed an interactive tool that enables users to view and compare relevant characteristics of the policies and terms and conditions that apply to users of digital platforms, terminal equipment and operating systems.

The tool also makes recommendations for consumer safety, such as encouraging consumers to ensure that applications and software are downloaded from official app stores and verify that the page is safe and reliable before making an online purchase, exercise caution when sharing photos and information, review privacy settings, alter passwords periodically, use different passwords on different digital platforms, and avoid lending mobiles and other devices with account information stored on them, as well as payment methods for digital services, to avoid misuse.

The comparator tool was awarded first prize in the 2023 annual good practices competition organized by the Latin American Forum of Telecommunication Regulators (REGULATEL), in the category of quality of service to the user. The Forum awards the prize annually to acknowledge best practices for the protection of user rights and quality of service at the international level.

[104] ITU-D Document https://www.itu.int/md/D22-SG01.RGQ-C-0183/ from Mexico

3.4.4 Seeking stakeholder feedback in Côte d'Ivoire[105]

To mark the tenth anniversary of the protection of personal data in Côte d'Ivoire, the data protection authority, the Telecommunication/ICT Regulatory Authority convened stakeholders to reflect on the implementation of Law No. 2013-450, relating to the protection of personal data, to formulate appropriate recommendations and to consider the outlook for development. The aim was to collect opinions and feedback on experiences and difficulties encountered by stakeholders (companies, administrations, firms, consumers, etc.) in the implementation of the law; subsequently, to compile recommendations with a view to future revisions of the legal framework; and lastly, to gauge the impact of the law on the various stakeholders. The comprehensive multistakeholder consultation on implementing rules is a regulatory best practice that may be emulated. Such laws can also be strengthened in terms of protecting the rights of especially vulnerable populations such as minors and persons with disabilities.

3.4.5 Discouraging dark patterns in India

The increasing online presence of consumers across multiple platforms and services leads to the disclosure and collection of vast troves of consumer PII, which can be analysed with the help of AI and used to deploy dark patterns that ultimately harm consumers.

The menace of dark patterns is especially relevant in developing countries where many consumers are first-time Internet users, even as they may be first-time users of mobile phones. In 2023 the Government of India released a draft, Guidelines for Prevention and Regulation of Dark Patterns, [106] to address the threat of harmful dark patterns.

The responsibility for a safe and fair digital world also rests with businesses to choose better business models, regulators who protect consumers, and consumers who must be aware of and assert their rights. However, consumer protection regulation should consider data protection establishing guardrails on how PII cannot be used. Such laws are valuable in a world where more detail is added to consumers' already comprehensive, oft-traded digital persona every time they log in.

Dark patterns are prohibited under the EU's Digital Services Act,[107] which acts in complements with other regulations, including the General Data Protection Regulation (GDPR) and the AI Act. The EU's Unfair Commercial Practices Directive seeks to prohibit unfair commercial practices affecting consumers' economic interests before, during and after the conclusion of a contract and has issued detailed guidance. The Consumer Protection Act in India also defines and bans unfair trade practices, which include deception. The guidelines on dark patterns are a step in this direction.

3.4.6 Deliberations on preventing the misuse of PII

The joint workshop with Question 6/1 ("Personal data usage: regulatory and economic aspects") which was held at ITU Headquarters in Geneva on 17 April 2024 highlighted the importance of safety, transparency, fairness, accountability, consumer education and choice regarding data usage and led to a number of useful insights.

---

[105] ITU-D Document https://www.itu.int/md/D22-SG01.RGQ-C-0177/ from Côte d'Ivoire

[106] https://consumeraffairs.nic.in/sites/default/files/file-uploads/latestnews/Draft%20Guidelines%20for%20Prevention%20and%20Regulation%20of%20Dark%20Patterns%202023.pdf

[107] https://digital-strategy.ec.europa.eu/en/policies/digital-services-act-package

A multistakeholder perspective to engender and maintain consumer trust: Aside from regulators, the industry, too, must be wary of the potential for blowback from consumers who reject exploitative technologies and harmful business models. While it is true that many consumers may not be aware that their data is being collected or misused, ultimately consumers will exercise their choice to preferentially adopt those technologies or business models that prioritize their safety and do not misuse their data. Innovation and competition are mechanisms to promote consumer-friendly digital services and preclude the need for excessive regulation.

Industry practices matter: Industry bodies such as the GSM Association are doing much to encourage good practices among their members. Multistakeholder cooperation is essential. Protective regulation, industry compliance and proactive consumer education were identified as the need of the hour.

Protection from misuse in the age of AI: As AI is trained on vast troves of data, consumer protection issues may arise, especially when such training and monitoring tools gather personal and sensitive data. There are risks associated with scraping public data sets that may include personal data; hence, it is crucial to have robust anonymization measures in place. There are risks of bias and discrimination, highlighting the need for transparency and consumers' right to be aware of the risks and limitations of AI models to enable them to make informed choices.

3.4.7 Best practices on enhancing consumer awareness and skills against misuse of PII

As digital technologies, particularly AI, continue to advance rapidly, the digital skills of both consumers and regulators are struggling to keep up. This lag intensifies the potential for consumer harm through online fraud, making it an urgent and pressing concern. A contribution[108] from RIFEN underscored the pressing need for cross-sectoral and global collaboration and capacity building in digital skilling to prevent further harm.

Considering the increase in the number of personal data breaches across the world in the last decade, informing the public and those consumers affected by such breaches will also contribute to preventing or reducing potential damages as well as raising the level of awareness on the misuse of PII. Operators in **Türkiye**[109] have a statutory obligation to report personal data breaches to the competent authorities and affected persons. In this regard, KVKK, the national data protection authority, has published a form for data controllers to use for personal data breach notifications. Furthermore, KVKK announces any data breach notifications deemed appropriate by the Board on its website.

The success of the digital economy and digital transformation depends on the efficient and effective use of massive amounts of data, a critical resource upon which innovative digital services depend.

Efforts to curb the misuse of PII and protect especially vulnerable consumers, as seen in the paragraphs above, are a work in progress as regulation catches up with rapid technology developments. Policy-makers worldwide should exercise great care when crafting guidelines that balance the protection imperative against the desire to reap the benefits of new technologies. Stakeholders must collaborate to protect consumers so as to engender and retain consumer

[108] ITU-D Document https://www.itu.int/md/D22-SG01.RGQ-C-0150/ from RIFEN
[109] ITU-D Document https://www.itu.int/md/D22-SG01.RGQ-C-0244/ from Türkiye

confidence for lasting digital transformation. Ultimately, it is vital to enhance consumers' skills and awareness so they can protect themselves against the misuse of PII.

Chapter 4 – Mechanisms to promote informed consumer decisions

4.1 National experiences with publishing transparent, comparable, adequate and up-to-date information pertaining to customer decisions on subscribing and terminating contracts for digital services

The telecommunication boom has led to a proliferation of products and services that facilitate people's work and life, entailing the widespread collection and use of personal data. This brings with it the challenge of ensuring that telecom consumers are still able to make informed decisions, that is to say autonomous decisions that are based on full awareness and are consistent with free and rational consumption behaviour. To achieve this, all stakeholders need to ensure that consumers have transparent, comparable, sufficient and up-to-date information available when purchasing, subscribing or terminating digital services. These efforts can be directed at legislation, data disclosure, practical tools, consumer education and service design.

4.1.1 Legislation and data disclosure to ensure consumers have access to transparent information

Both a healthy market and the protection of rights and interests require that the information asymmetry between operators and suppliers on the one hand and consumers on the other be minimized. This can be achieved through public disclosure of relevant data, by releasing investigation reports and other key information, and by standardizing legislation and regulatory texts on consumer rights and interests. This should strengthen the oversight of operators and service providers, enhance market transparency and effectively safeguard consumers' right to be informed.

India has amended and strengthened its legislation on electronic transactions to prohibit unfair trading practices in e-commerce, safeguard consumers' interests and guarantee that e-commerce platforms are transparent.[110]

South Africa has clamped down on false advertising through legislation. The Consumer Protection Act 68 regulates the provision of goods and services, the conclusion of consumer contracts and the promotion and marketing of goods and services. It also protects consumers against false and misleading attempts to induce consumers to enter unfavourable contracts.[111]

In the **United Kingdom**, the independent communications regulator Ofcom publishes the majority of its survey data in an open format, enabling stakeholders to download and analyse the data. This is in addition to the publication of data tables, technical reports and field materials. The regulator sees this practice reflected in industry responses to consultations, including on topics like switching.[112]

---

[110] ITU-D Document https://www.itu.int/md/D22-SG01.RGQ-C-0004/ from Liberia
[111] Ibid
[112] ITU-D Document https://www.itu.int/md/D22-SG01-C-0237/ from United Kingdom

In **China**, the Information and Communication Administration of the Ministry of Industry and Information Technology is the regulatory agency for the telecommunications industry. It is responsible for setting and promulgating standards and management measures related to telecommunications service quality, monitoring their implementation, as well as monitoring quality issues in telecommunications services and disclosing the handling process and results of major service quality events to the public.[113]

The telecom operator China Mobile fully displays all tariff plans in prominent positions, including physical stores and the China Mobile app, highlighting key information such as terms, scope and duration of promotions.[114]

In **Madagascar**, where subscription to services and contract termination are a common cause for complaints, a customer information space was established on the ARTEC website and an infrastructure map was published showing 2G, 3G and 4G coverage in Madagascar.[115]

In **Türkiye**, BTK has introduced a regulation on the procedures and principles for electronic contract termination services through the e-government gateway. This initiative will contribute to more effectively protecting consumers. Not only does it enable consumers to cancel their contracts more easily and quickly, it also keeps them informed throughout the contract termination process. An electronic contract termination service with multi-factor authentication also provides protection against abuse and fraudulent transactions, thus enhancing security and trust.[116]

4.1.2 Practical tools to assist consumers' access to comparison information

The proliferation of rapidly changing products and services often makes it difficult for consumers to make comparisons in terms of substance and value. In response to the complex and dynamic market environment, stakeholders can collaborate to create information tools to provide consumers with the necessary information, helping them make more informed and efficient decisions.

In the **Democratic Republic of the Congo**, ARPTC has established a web portal for consumers to simulate and compare prices of telecommunication services available on the market, so they can choose the services that best suit their needs and estimate the required budget. Additionally, ARPTC has released a tool to audit subscriber contracts offered by MNOs, identifying dubious conditions that may infringe on the rights of consumers.[117]

The Federal Telecommunications Institute of **Mexico** has implemented various information mechanisms for users of telecommunications services so as to enhance their rights and foster the growth of an innovative digital environment that is safe and fosters trust. These initiatives include online tools and information resources, including a comparator for telecom plans and rates, a tool for selecting the best plan based on one's usage profile (*Conozco mi Consumo*), a mobile device comparator, and reports comparing plans and rates for a variety of telecommunication services. These tools and resources empower consumers to make better-informed decisions

[113] ITU-D Document https://www.itu.int/md/D22-SG01.RGQ-C-0222/ from China Mobile Communications Corporation
[114] Ibid
[115] ITU-D Document https://www.itu.int/md/D22-SG01.RGQ-C-0028/ from Madagascar
[116] ITU-D Document https://www.itu.int/md/D22-SG01-C-0345/ from Türkiye
[117] ITU-D Document https://www.itu.int/md/D22-SG01.RGQ-C-0031/ from the Democratic Republic of the Congo

about their telecommunications services by facilitating comparison, diminishing information asymmetries, and boosting user empowerment.[118] The Federal Telecommunications Institute has created an electronic catalogue of Internet of Things devices that comply with technical regulations, providing transparent information about privacy policies and device characteristics and enabling users to make informed decisions and use IoT equipment properly.[119] The Federal Telecommunications Institute has also developed an interactive tool providing information on the policies, terms and conditions of digital platforms, with an interactive application for users of digital services. The tool highlights what information users share with the platforms and how that information is handled, and outlines the scope of the permissions that users grant to these platforms.[120]

In **Romania**, the national telecommunication authority ANCOM has developed several platforms (Veritel, Netograf) which allow users to compare tariffs and measure the quality of Internet access services provided by different operators. Access to comparable, adequate, and up-to-date information through such tools helps end users make informed choices when purchasing and using electronic communications services.[121]

4.1.3 Using consumer education and service design to help consumers get access to comprehensive and up-to-date information

Targeted and content-rich training activities can enhance the ability of consumers to obtain information, assess their self-protection and get access to the latest market trends and information. Service design, too, can help ensure that consumers are able to make well-informed purchasing decisions: an example is an efficient and transparent subscription system that lets consumers obtain sufficient and detailed product and service information.

In **Mexico**, the Federal Telecommunications Institute publishes reports on the terms and conditions of e-commerce platforms[122] and on the protection of their users' private information,[123] providing clear, simple and transparent information about the platforms' policies in this domain. The Institute has identified deficiencies related to contract termination.

The **Côte d'Ivoire** Telecommunications Regulatory Authority has implemented a model for permanent proximity centres for education and treatment of consumer complaints (CPP-ETRC), specifically aiming to inform and train consumers on technological advances in ICTs and their rights as users of ICT products and services and to hold regular training and information activities on new digital technologies and on changes in consumer rights.[124]

The telecom operator **China Mobile** has implemented a two-step confirmation system for subscriptions, prompting consumers for confirmation when considering signing a contract by means of SMS or a hotline. For consumers using app services, it proactively provides information such as the "Personal Information Collection Manifesto" and "Third-Party Information Sharing List", and informs consumers about the fields, business scenarios, collection purposes, methods, as well as how to access, correct and delete personal information.[125]

---

118 ITU-D Document https://www.itu.int/md/D22-SG01-C-0071/ from Mexico
119 ITU-D Document https://www.itu.int/md/D22-SG01.RGQ-C-0097/ from Mexico
120 ITU-D Document https://www.itu.int/md/D22-SG01.RGQ-C-0183/ from Mexico
121 ITU-D Document https://www.itu.int/md/D22-SG01-C-0478/ from Romania
122 ITU-D Document https://www.itu.int/md/D22-SG01.RGQ-C-0100/ from Mexico
123 ITU-D Document https://www.itu.int/md/D22-SG01.RGQ-C-0099/ from Mexico
124 ITU-D Document https://www.itu.int/md/D22-SG01-C-0118/ from Côte d'Ivoire
125 ITU-D Document https://www.itu.int/md/D22-SG01-C-0222/ from China

ITU-D held a joint workshop on mechanisms for enhancing consumer awareness to promote informed consumer decision-making. The workshop brought out best practices in the area of consumer protection, awareness and empowerment as well as mechanisms to address cybersecurity and online safety issues, with the overarching goal of strengthening consumer protection and awareness in the digital era. Key points included improving infrastructure in underserved areas, enhancing security and developing digital skills.[126]

4.2 Transparency on billing, including third-party payments such as direct carrier billing, premium-rate services and mobile payments

The ongoing dynamism of the telecommunication sector also represents a challenge for regulators concerned with transparency relating to the evolution of telephone bills. Direct carrier billing (DCB), in the past used by operators primarily to charge for telecommunication services provided to customers, have become a means for third-party providers to charge their customers for the purchase of other products and services.[127]

DCB offers notable advantages. For MNOs, it represents an opportunity to create additional revenue streams. On the consumer side, DCB is a convenient method of paying for purchases or subscriptions using the mobile bill or prepaid balance as an alternative to cash and cards.

However, the DCB model faces a big challenge in the shape of the risk that consumers may unintentionally subscribe to value-added services or make purchases without fully understanding the terms, prices, and cancellation procedures.[128]

Given that a high proportion of consumer complaints in the sector is related to billing and payments,[129] consumer protection mechanisms, including billing transparency, are important tools for regulators and service providers to consider.

In **China,** telecom operator China Mobile informs its customers about their remaining consumption credits, with alerts to avoid unnecessary charges at specific times of the month, or when consumption exceeds a specified threshold. It also provides convenient query services, allowing consumers to enquire about current service status, available resources, bills and other information through hotlines, SMS, WeChat, and other applications and channels.[130]

Telecom customers in China can also view their bills in real time and access detailed records, dating back at least 12 months, in the operators' application. They can also review their service agreements, compare voice/SMS/data usage across periods, and receive automatic alerts for data overuse, ensuring transparent consumption management and traffic management.[131]

After a sharp increase in complaints related to mobile payment fraud, **Uganda** has introduced measures such as SIM card registration and SIM swap obligations, and begun offering consumer awareness campaigns and regular cybersecurity empowerment programmes in collaboration

---

126 ITU-D Document https://www.itu.int/md/D22-SG01-C-0335/ report of the workshop on increasing consumer awareness mechanisms to promote informed consumer decision (joint workshop for Question 6/1 and Question 3/2 held in Brasilia from 18-20 June 2024)
127 BoR (21) 118. BEREC Report on the handling of third-party payment charges on mobile phone bills
128 ITU-D Document https://www.itu.int/md/D22-SG01.RGQ-C-0059/ from Türkiye
129 ITU. Digital Regulation Handbook. Geneva, 2020
130 ITU-D Document https://www.itu.int/md/D22-SG01-C-0222/ from China
131 ITU-D Document https://www.itu.int/md/D22-SG01-C-0507/ from China

with relevant stakeholders. These measures have contributed to curbing mobile money fraud and promoted consumer safety.[132]

Some regulators have introduced specific measures for prepaid consumers, since it is easier for a post-paid user to check a bill than for a prepaid one to check the credit balance before and after each transaction. Thus, telecom operators in **India** have the obligation to provide the following information to prepaid consumers by SMS after the activation of any service involving a value-added service (VAS): amount deducted, purpose, balance, and validity period of the value-added service.[133]

A notification mechanism set up by BTK regulation in **Türkiye** creates the following obligations:

a) All operators must notify their subscribers when the usage of each service in their tariff plans (calls, texts and data) reaches certain thresholds, set by the regulation as 80 per cent and 100 per cent.
b) Operators having more than 200 000 subscribers are also obliged to notify their subscribers when the total amount of charges (including third-party payments) against the monthly bill reaches 100 Turkish liras, or a limit defined by the subscriber.[134]

Notifications based on the volume and financial limits specified in the BTK regulation are sent to all subscribers unless otherwise requested. The regulation aims to increase billing transparency, protect subscribers against bill shocks and allow them to better control their usage of services and expenditures. Faced with a surge in complaints about value-added services, BTK also issued its VAS Principles, a set of rules intended to provide transparency at all stages of subscriptions and purchases related to value-added services and ensuring that consumers are fully informed about the terms and conditions of the services, including pricing. To this end, the VAS Principles established detailed and separate procedures for services purchased via the Internet, SMS, and phone call channels.[135]

Finally, according to the European Electronic Communications Code (EECC), end users are often not aware of the cost of their consumption behaviour or have difficulties in estimating their time or data consumption when using electronic communications services. Thus, in order to increase transparency and to allow for better control over bills, countries should be able to maintain or introduce provisions on consumption limits protecting end users against bill shocks, including in relation to premium-rate services and other services subject to particular pricing conditions.

BEREC, in its strategic plan, emphasizes that regulators still have an important role to play in ensuring consumer transparency, even though digitalization has empowered consumers, and remains committed to monitoring the digital sector and promoting increased transparency so that consumers can make informed decisions.[136]

Transparency measures become even more important for roaming consumers, as value-added services can lead to higher bills when used abroad. To increase transparency in such situations,

---

132 ITU-D Document https://www.itu.int/md/D22-SG01.RGQ-C-0046/ from Uganda
133 ITU and the World Bank, Digital Regulation Platform, Protection of consumers with prepaid accounts
134 ITU-D Document https://www.itu.int/md/D22-SG01-C-0236/ from Türkiye
135 ITU-D Document https://www.itu.int/md/D22-SG01.RGQ-C-0059/ from Türkiye
136 BoR (20) 108. BEREC strategy 2021-2025.

new measures have been introduced by Regulation (EU) 2022/612 ("Roaming Regulation") recasting Regulation (EU) No 531/2012 which expired on 30 June 2022.[137]

In summary, despite the many advantages offered by the growing number of third-party services and the mobile payment they use – financial inclusion, customer convenience etc. –consumers are often unaware of the costs they can incur. This is because, firstly, they lack sufficient information on the terms and conditions applicable to those services, including pricing, and secondly because of the new fraud risk associated with mobile payments. These considerations make billing transparency and consumer awareness in the electronic communications sector more important than ever.

4.3 Best practices for consumer protection measures related to quality of service/experience, and security of services offered to consumers

Although telecommunication services have become eminently accessible and participation in the digital ecosystem extremely widespread, the digital skills and digital literacy they require remain very unevenly distributed, hampering full participation and safe, informed use of the different services.

Therefore, it is important that the regulatory authorities of the telecommunications sector implement programmes to promote digital literacy and consumer protections for the safe use of Internet access and digital platforms among consumers; as well as making available transparent information about the terms and conditions to which users are subject when using the different services for better decision-making when accessing and using these services.

For example, **Liberia**[138] has highlighted growing concerns about the need to protect consumers against poor quality of service and misleading advertising, noting that political dialogue will be needed. In the absence of adequate legislation, consumers are increasingly vulnerable to online fraud. It is recommended that consideration be given to prohibiting unfair trading practices in e-commerce, safeguarding consumer interests and ensuring that e-commerce platforms are transparent. In addition, legislation should be strengthened to legally enshrine the rights of customers and the obligations of service providers.

Also noteworthy is the experience of **Uganda**, the strategies adopted and the results achieved by the regulator in collaboration with key stakeholders such as MNOs and the Central Bank of Uganda to curb mobile money fraud and promote consumer safety.[139]

Among the results that might be mentioned are increased consumer awareness and self-efficacy, leading to a reduction in cases of mobile money scamming, increased consumer confidence in digital financial services, and growth in mobile money subscribers.

This experience shows how improving user trust can go hand-in-hand with greater adoption of digital services. Digital literacy is one of the main determinants of consumer security, and consumer empowerment builds self-efficacy, confidence and security in the use of mobile money applications.[140]

---

137 BoR (22) 174. BEREC Guidelines on Regulation (EU) 2022/612 and Commission Implementing Regulation (EU) 2016/2286 (Retail Roaming Guidelines).
138 ITU-D Document https://www.itu.int/md/D22-SG01.RGQ-C-0004/ from Liberia
139 ITU-D Document https://www.itu.int/md/D22-SG01.RGQ-C-0046/ from Uganda
140 Ibid

Another good illustration is to be found in the report from **Mexico**, where the terms and conditions of e-commerce platforms have been analysed and summarized so that users are informed about the conditions that apply to them when using the platforms or doing transactions through them.[141]

The most relevant information is synthesized and grouped into variables such as: provider's responsibility towards users, billing, transactions and payment methods, complaints, return policies.[142]

Informing users is viewed as essential for promoting informed and responsible use of digital platforms and thus the effective participation of the population in the ecosystem.[143]

Privacy is another important aspect of platform use that users need to understand, given the amount of information that is shared through the various digital platforms. For this reason Mexico analyses privacy policies so that users can easily inform themselves about the information they share, the retention time, with whom their information is shared and the permissions granted to the platforms on the content they generate, among other details[144].

The user privacy reports for digital platforms include the privacy policies embodied in operating systems, terminal equipment, social networks and digital platforms that enable the provision of services such as: online commerce, transportation, entertainment, etc.[145]

Consumer protection is an important part of building consumer trust, which is a crucial factor in the continued adoption of new technologies. This is particularly true in an ever more interconnected world of telecommunications networks and information technology. The role of regulators in analysing protections and verification how the rights of users are protected is therefore a vital one.

Thus, regulatory authorities should supervise and regulate consumer rights pertaining to access, quality of service, pricing and competition

In this regard, the actions taken by the **Republic of the Congo** stand out. The contribution presents the results of an analysis of the measures adopted by telecommunications regulators to protect consumers in the digital environment and provides a set of proposed guidelines based on their experience and analysis.[146]

Service quality

- Ensure that services provided are of a quality consistent with applicable standards, particularly in terms of availability, reliability and connection speed.
- Establish mechanisms for monitoring and measuring service quality, as well as procedures for the swift resolution of technical issues.

141 ITU-D Document https://www.itu.int/md/D22-SG01.RGQ-C-0100/ from Mexico
142 Ibid
143 ITU-D Document https://www.itu.int/md/D22-SG01.RGQ-C-0099/ from Mexico
144 Ibid
145 ITU-D Document https://www.itu.int/md/D22-SG01.RGQ-C-0100/ from Mexico
146 ITU-D Document https://www.itu.int/md/D22-SG01.RGQ-C-0147/ from the Republic of the Congo

Online transaction security

- Implement robust security measures to protect online transactions, including strong authentication and encryption of confidential data.
- Educate consumers about the risks of online fraud and provide them with advice on the best ways to protect their information.
- Adopt stricter security standards and protocols to protect online transactions against fraud and piracy.
- Promote the use of secure payment technologies, including tokenization and strong authentication.

Promotion of accessibility, education and awareness

- Encourage companies to make their platforms and user interfaces more user-friendly and accessible to all users.
- Implement awareness and education programmes for consumers about their rights and best practices in online security.
- Promote digital literacy to enhance consumers' skills in navigating safely in a digital environment.

Côte d'Ivoire has implemented a project involving permanent centres to establish a framework of proximity among consumers, administrative authorities and protection agencies, aiming to foster a trust ecosystem.[147]

These permanent centres have specific objectives, including informing and educating consumers about advances in ICTs and their rights related to the use of ICT products and services, establishing mechanisms for collecting and processing consumer complaints for non-compliance with current regulations, periodically conducting training and informational activities on new digital technologies and the evolution of consumer rights.

In **China**, it has been observed that ensuring consumers are well informed when making decisions benefits both consumers and businesses, leading to a more sustainable economy and a safer and more reliable environment.[148]

Among the mechanisms that China has shared and implemented in protecting rights and interests of telecommunication consumers is the ongoing, continuous improvement of legislation and regulations to provide a legal basis for the protection of those rights.

It is essential for regulatory bodies to keep pace with the development of the ICT industry, improving and refining regulatory measures to ensure that informed consumer decision-making is protected in a manner that is more comprehensive, timely and targeted.

4.4 Transparency requirements for traffic management and zero-rating practices based on current national experiences

The explosion in digital technologies and telecommunication services mentioned above has been accompanied by a boom of connectivity, rights, and the development of essential activities

[147] ITU-D Document https://www.itu.int/md/D22-SG01-C-0118/ from Côte d'Ivoire
[148] ITU-D Document https://www.itu.int/md/D22-SG01-C-0222/ from China

in the digital environment. According to the ITU report "Facts and Figures 2024", the number of people in the world using the Internet today is estimated at 5.5 billion.[149]

Traffic management and zero-rating practices, which can be implemented for reasons such as service quality, network optimization, security, fair-use policy, commercial interests etc., can have negative impacts on consumers when they are implemented in a non-transparent and discriminatory manner. Making consumers aware of the terms and conditions attached to such services is far from straightforward. Nonetheless, zero-rating can be beneficial to many public and private organizations and consumers. For example, in the public sector zero-rating services can help to reduce cost, gain time and increase engagement in education, health and digital government services.[150]

Colombia[151] has had a regulation on the issue since 2011. The regulation stipulates that, in respect of the right to free access to the Internet, service providers cannot generate any type of blocking, discrimination or preference to any particular company, application or specific content to the detriment of another. The only content that might be restricted are those determined by law, such as violence or gambling, which is taken into consideration in a special way by service providers. Service providers are also entitled to take measures to avoid traffic congestion. Finally, the regulation obliges operators to give complete and transparent information to the users concerning conditions of the tariff plans, including whether they have additional, no-cost applications. During the pandemic, the regulatory authority developed measures to allow health and education institutions to benefit from zero-rating offers to give consumers access to basic everyday information at no cost, for purposes of social welfare.

4.5 Best practices on mechanisms to promote informed consumer decisions

In summary, there is a range of measures that can be taken to ensure that consumers are able to make more informed decisions and to empower them to advocate for their own rights and interests. The overall thrust is to increase their level of knowledge and awareness of ICT and telecommunication services and strengthen their confidence in using them. This can include the following:

1. Make general information, reports, research, guides, and other tools on consumer-related issues available online to encourage and empower consumers to engage successfully with telecommunication/ICT.
2. Ensure that clear, comprehensible and transparent information is provided about the contracts and terms and conditions to which users are subject when utilizing telecommunication services and digital platforms.
3. Create practical tools such as network coverage maps, information portals, comparison websites for tariff offers, and product and service information so that consumers are able to make well-informed, sound decisions.
4. Increase transparency and consumer awareness regarding billing for telecommunication services to help consumers better control their usage of services and make informed decisions, especially for subscriptions or purchases related to third-party services.

---

149 Facts and Figures 2024. https://www.itu.int/itu-d/reports/statistics/2024/11/10/ff24-internet-use/

150 ITU-D SG1 Document https://www.itu.int/md/D22-SG01-C-0335/en Report of the workshop on Increasing Consumer Awareness Mechanisms to Promote Informed Consumer Decision: A joint workshop for Question 6/1 and Question 3/2 held in Brasilia from 18-20 June 2024.

151 Ibid

5. Put in place technical and organizational measures for mobile payments to address consumer concerns about abusive or fraudulent practices.
6. Where mobile payment is a cross-sectoral issue and poses regulatory challenges, encourage cooperation and collaboration between competent authorities and other stakeholders.
7. Ensure that services provided are of a quality consistent with applicable standards, particularly in terms of availability, reliability and connection speed.
8. Establish mechanisms for monitoring and measuring service quality, as well as procedures for the swift resolution of technical issues.
9. Ensure that telecommunications and digital service providers implement robust security measures to build confidence and enhance consumers' protection, information and safety when accessing the Internet and digital platforms, including awareness and education programmes for consumers regarding their rights and best practices in online security.
10. Regarding traffic management and zero-rating practices, ensure that users are provided comprehensive information including tariff terms, data consumption, free services/applications eligibility and terms, and applicable conditions.
11. Coordinate with service providers on zero-rating telecommunications to enable free access to certain public services.

Chapter 5 – Measures adopted to stimulate protection of consumers, in particular vulnerable users

We have seen how important consumer protection is in the digital world; this is the case for vulnerable users in particular. It starts with the need to facilitate accessibility, frequently a major problem for persons with disabilities or special needs. While developed countries often have solutions in place to promote the equality of people, in line with the Universal Declaration of Human Rights, people in developing countries often face quite formidable challenges.

Among the above-mentioned solutions that have been implemented in different countries, the following may be mentioned:

- Voice-to-text conversion for the hearing impaired.
- Scalable font size or text-to-speech conversion for persons with visual impairments, failing or degraded eyesight.
- Warning, space awareness and motion sensors for people with poor or limited eyesight.
- Digital libraries for those who are deaf or hard of hearing.
- Global positioning system (GPS) navigation for persons at particular risk of getting lost.
- Digital photo albums and voice recordings for people with amnesia, dementia or short-term memory loss to remind them of their past and the identity of their friends and relatives.
- The prospect of independent mobility through self-driving cars for the blind or visually impaired, in the future.
- Devices producing sentences to enable people with, for example, motor neuron disease, who can no longer speak, to communicate.

For developing countries, the situation remains complex because of the limited availability of training and equipment.

In those countries, much of the work of promoting the independence of persons with disabilities and developing practical solutions to meet those needs within a context of limited resources is done by disabled persons' organizations (DPOs). Thus, government agencies should seriously consider supporting and promoting the work of DPOs and other NGOs as a primary strategy for addressing the issue of accessibility. This could lead to immediate results, thanks to a direct relationship with the beneficiaries and the existence of a basic resource infrastructure, with trained and qualified personnel to meet the needs expressed. In **China**, telecom operator China Mobile is driving the comprehensive upgrade of older person-friendly services across service scenarios, service depth, and solution innovation through measures such as: AI-powered digital entertainment services tailored for seniors, health platforms with embedded AI family doctors, and exploratory solutions in eldercare robotics.[152]

Meanwhile, China is continuously promoting the deep integration of digital technology and education. Firstly, China continues to accelerate 5G network deployment, which ensures reliable network support for emerging teaching scenarios. Secondly, China is committed to extending

[152] ITU-D Document https://www.itu.int/md/D22-SG01-C-0503/ from China

digital education hardware, applications and services to households and rural areas, which provides high-quality learning resources and online tutoring for pupils and providing parents with education support.[153]

China Mobile has also actively explored the application of 5G technology in the medical field to provide high-quality medical resources to remote areas, making public health services and patient care more accessible and more efficient.[154]

5.1 Best practices to ensure quality, information and security of members of economically disadvantaged communities, persons with disabilities, older persons, women and children

In an analogous manner, the contribution of **Côte d'Ivoire** on question 7/1 gives an inventory of the accessibility of telecommunications/ICT for persons with disabilities in developing countries, particularly in Côte d'Ivoire, and proposes strategies for effective inclusion. Thus, like any developing country, Côte d'Ivoire also faces several problems at the same time: illiteracy, lack of digital skills, low income and communication difficulties.

To remedy this, it proposes a list of solutions that can be implemented by Member States in order to achieve full inclusion and give everyone the opportunity to benefit from the digital transformation:

- Develop knowledge for policy-makers and decision-makers on ICT accessibility in order to facilitate the formulation and implementation of related ICT accessibility policies and strategies.
- Develop knowledge to assess and monitor the implementation of ICT accessibility across sectors and at national level.
- Develop the guidelines and related roadmap for implementation to ensure that e-government products and services are digitally accessible to all without any discrimination of gender, age, ability to use technology or level of education.
- Share good practices on the implementation of national ICT accessibility policies, legal frameworks, guidelines, guidelines, strategies and technological solutions to improve accessibility, compatibility and usability of telecommunication/ICT services.
- Facilitate the implementation of accessible e-government and other socially relevant digital services.
- Facilitate the financial accessibility of new accessible (smart) and emerging technologies.
- Ensure that ICTs, in particular those relating to emergency and crisis situations, are designed and disseminated in accessible digital formats, so that information is accessible to all, including disabled people. Encourage the education and training of persons with disabilities and persons with special needs in the use of telecommunications/ICTs, and the education and training of persons with disabilities in the use of telecommunications/ICTs.
- Encourage the education and training of experts responsible for helping persons with disabilities and persons with special needs to use telecommunications/ICTs.
- Promote the use of accessible telecommunications/ICTs to promote the employment of persons with disabilities in order to guarantee an open and inclusive society.
- Develop mechanisms to involve persons with disabilities and persons with specific needs in the process of developing legal/regulatory provisions, public policies and standards relating to telecommunications/ICT accessibility: creation of a platform exchange.

[153] ITU-D Document https://www.itu.int/md/D22-SG01-C-0504/ from China
[154] ITU-D Document https://www.itu.int/md/D22-SG01-C-0506/ from China

– Develop knowledge aimed at ensuring the design and development of physical digital environments (e.g. smart cities and towns) at the national level are accessible and inclusive for all people, including persons with disabilities.

In Cameroon, the EmpowerBlind initiative is taking a proactive and inclusive approach aimed at transforming digital divide into development opportunities. The objective of the project is to measure the blind and visually impaired youth's relationship with technology, assess their level of digital skills, and identify possible barriers to their inclusion in the ICTs.[155]

[155] ITU-D Document https://www.itu.int/md/D22-SG01-C-0541 from Cameroon

Chapter 6 – Conclusions

6.1 Summary of key findings

The studies conducted under ITU-D Question 6/1 (2022-2025) have identified key advances in consumer information, protection and rights within an evolving digital ecosystem. The findings emphasize the growing complexity of digital interactions and the increasing need for proactive complaint-handling *systems* and consumer-centric regulatory frameworks. The key takeaways include:

- Digital transformation and consumer protection needs:
  - The expansion of telecommunication and ICT services has provided consumers with greater access to digital services but is also a potential source of risks involving online fraud, misuse of their PII, and misleading digital transactions.
  - Emerging risks, such as dark patterns, unfair contract terms and manipulative marketing, call for regulatory interventions.
  - Consumer trust in digital platforms is contingent upon transparent, accountable and enforceable regulations that balance innovation with consumer protection measures and enhanced focus on trust and accountability.
- Regulatory challenges and responses:
  - Regulatory frameworks are often outdated, lacking adaptability to address risks associated with AI, IoT and automated decision-making systems.
  - Many countries have introduced adaptive regulatory approaches, including cross-sector collaboration, data-driven policy-making, and increased consumer education.[156]
  - Co-regulation and industry self-regulation have gained prominence, allowing voluntary compliance mechanisms to complement traditional enforcement tools and respond more promptly to industry evolution.
- Consumer education and awareness:
  - Digital literacy and awareness programmes are critical for mitigating risks associated with fraud, misuse of PII, and unethical digital marketing practices.
  - Several national initiatives have successfully enhanced consumer participation by providing interactive tools and transparent complaint resolution mechanisms.
- International collaboration:
  - The cross-border possibilities of digital commerce underscore the value of cross-border collaboration.

6.2 Policy guidelines

Based on the findings, the following policy guidelines are proposed to strengthen consumer protection and promote an inclusive, transparent, and accountable digital ecosystem:

- Establishing fit-for-purpose regulatory frameworks
  - Develop technology-neutral regulations that can adapt to emerging consumer risks while supporting innovation.
  - Implement risk-based regulatory approaches that focus on high-risk areas such as preventing fraud and misuse of PII and promoting transparency in digital transactions.

[156] https://app.gen5.digital/benchmark/concepts

- Enhancing transparency, consumer digital literacy and empowerment
    - All stakeholders should support better-informed decision-making where consumers have transparent, comparable, adequate and up-to-date information about the terms and conditions of services to which consumers are subject when accessing, using or terminating the services.
    - Governments and regulatory bodies should invest in consumer awareness programmes that educate the public on cybersecurity and fair contract terms.
    - Encourage interactive digital tools, such as a complaint tracking systems and telecom service comparison platforms, to empower consumers with real-time insights.
- Strengthening enforcement and compliance monitoring
    - Deploy automated monitoring systems to detect online fraud, misleading advertising and data misuse.
    - Implement proactive compliance audits to ensure adherence to consumer protection laws, particularly in digital marketplaces and financial transactions.
- Fostering international collaboration and cross-border regulatory consistency
    - Collaborate internationally to enhance consumer protection measures across jurisdictions.
    - Strengthen partnerships among relevant public bodies to combat cross-border online fraud and misuse of PII.
- Promoting ethical business practices in digital markets
    - Encourage businesses to adopt transparent terms of service and opt-in policies for consumer data usage.
    - Develop industry-led codes of conduct to ensure fair competition and consumer transparency.
- Expanding protection for vulnerable consumer groups
    - Implement policies that address the needs of older persons, persons with disabilities and economically disadvantaged communities.
    - Promote inclusive design in digital services to ensure equal access to essential telecommunications and ICT resources.

6.3 The path forward

The discussions under ITU-D Question 6/1 (2022-2025) and the resulting findings reaffirm the critical role of consumer information, protection, and rights in fostering trust, inclusivity and sustainability in the digital economy and society. As digital transformation accelerates, ensuring a secure, fair and equitable environment for all consumers, particularly vulnerable groups, remains an urgent priority.

Future research should build on these findings and adopt holistic, multistakeholder approaches involving governments, industry players, academia and civil society, prioritizing proactive regulatory adaptation, global collaboration, and consumer empowerment to ensure that digital transformation remains consumer-friendly, inclusive and sustainable. Key research areas may include:

- Behavioural science in regulatory design: Leverage nudging techniques and consumer decision-making insights to improve digital literacy and fraud prevention and PII protection.

- Algorithmic transparency: Understanding and promoting accountability in automated decision-making.
- Cross-jurisdictional regulatory cooperation: Strengthen cross-border cooperation to continually enhance consumer protection frameworks.
- Regulatory toolkit development: Create evidence-based guidelines covering data protection, transparency and ethical business practices.
- Emerging technologies for consumer protection: Explore how new and emerging technologies can enhance consumer protection, streamline complaint resolution and prevent online fraud.
- Capacity building for policy-makers and regulators: Equip regulatory authorities with the skills and tools necessary to address the evolving landscape, ensuring continued consumer trust and safety.

Annex 1 – Case studies

1.1 Cooperation and information-sharing among policy-makers, regulators and consumer associations

Côte d'Ivoire – Consumer Council

The Consumer Council created by ARTCI is an inclusive exchange framework that integrates all stakeholders to protect the rights of consumers of telecommunications/ICT services in domains that fall within the remit of ARTCI: electronic transactions, protection of personal data and privacy, and the fight against cybercrime. Concretely, the Consumer Council formulates opinions, proposes draft decisions and makes recommendations to the ARTCI Regulatory Council, taking into account technological, economic and regulatory developments. This is done either at the request of the ARTCI Regulatory Council or on the initiative of the Consumer Council, in an anticipated or proactive manner, on matters regulated by the ARTCI. Consumer associations are appointed to the Consumer Council for a renewable period of two years, following a selection procedure based on transparent criteria set by decision of the ARTCI Regulatory Council.

Democratic Republic of the Congo

The collaboration mechanism between ARPTC and the consumer associations is intended in particular to inform consumers about current news and trends in ICT, identify the problems consumers face, and inform them of the remedies available. To set up the collaboration mechanism, ARPTC identified three associations having a particular impact on the population, one of which specialized in the ICT sector.

Côte d'Ivoire – permanent local centres

The aim of creating permanent local centres for education and processing consumer complaints is mainly to promote proximity between consumers and administrative and protection authorities, promoting an ecosystem of trust. These centres will have the following specific objectives:

- inform and train consumers on technological advances in ICT and on their rights related to the use of ICT goods and services.
- set up mechanisms for collecting and processing malfunctions and complaints related to non-compliance with standards in force, reported by consumers.
- conduct regular training and information activities on new digital technologies and on the evolution of consumer rights.
- provide alerts to administrations and regulators in order to promote revisions and adjustments of standards and structures.
- be a digital observatory.

In view of the objectives pursued, the results of the work of these centres should be able to contribute significantly to strengthening the protection of consumer rights and contribute to reducing the digital divide.

1.2 Mechanisms/tools for listening to the consumer and means to receive and resolve consumer complaints

Türkiye – Online complaint notification

The Information and Communication Technologies Authority of Turkey, BTK, has established an online complaint notification system to resolve consumer/user complaints in electronic communication and postal services. By dispensing with paper-based and post-reliant processes, this contributes to the country's digital transformation processes. The system offers multiple levels of appeal, improving the chances of resolution at the source (without the direct intervention of BTK) and thus reducing the Authority's workload. Registered complaints can serve as an input for possible regulatory and supervisory action. Finally, the system facilitates the classification and analysis of consumer complaints to identify particularly problematic issues and provides an opportunity to take quick action.

Nigeria – Complaints channels and consumer engagement

The National Communications Commission (NCC) of Nigeria has come up with two strategic initiatives, focussed on complaint channels and consumer engagement respectively, to ensure the protection of digital consumers. One initiative is the Telecom Consumer Parliament, "a high-level dialogue forum held twice a year to address critical and contemporary issues affecting the Nation's telecommunications industry during which key telecom industry players gather to exchange ideas on salient issues affecting the consumers of telecommunication services in Nigeria". The other is Telecom Consumer Conversations, which consists of various interactive programmes including Telecom Campus Conversation, NYSC Camp Sensitization, Village Square Dialogue, and Market Conversation. Through the initiatives described above and many other public actions and measures, it has been possible to progressively reach out to a large number of Nigerians, particularly at the grass-roots level, to ensure that the public fully understands and appreciates the benefits of telecommunication services and to enlighten and inform them about their rights.

China

In China, operators have a mandate to optimize market service initiatives to promote consumer-informed decision-making. China Mobile gathers consumer feedback through complaint hotlines and through its customer service. The end goal is to ensure the service quality for all telecom consumers and informed decision-making b consumers, for total consumer satisfaction.

An important stakeholder is the China Consumers Association (CCA), a nationwide social organization that safeguards the legitimate rights of consumers. It accepts complaints, conducts investigations and offers consultation services to consumers, including litigation. It publicizes unfair and non-transparent behaviour of enterprises, as well as activities which violate consumer's rights and interests. National live broadcasts are held annually. These are highly public events that serve to expedite resolution of issues and provide added motivation for self-scrutiny by telecom enterprises and service providers and improvements to consumer information.

Democratic Republic of the Congo

ARPTC has designed numerous tools to contribute to better consideration of consumer rights. One is CEIR , a national system to combat the theft and counterfeiting of mobile terminals that

can help consumers recover their lost or stolen terminals. Another is the web portal created by ARPTC to handle complaints from consumers of digital services. This website also serves as a price simulator and market comparator to help consumers choose the offer best suited to their needs and determine assess the necessary budget. Some tools have been designed in collaboration with consumers of digital services, including a toll-free centralized hotline. Building on the successful collaboration and dialogue between the telecoms regulator and consumers, ARPTC is planning the following additional initiatives: the creation of a discussion forum on Facebook for exchanges with digital consumers on their concerns related to the provision of digital services; a tripartite charter between MNOs, ARPTC and digital consumers' associations; and surveys among households to measure the level of satisfaction with the services of the MNOs.

Haiti

The regulator in Haiti has created a unit for monitoring operators for the benefit of customers. The regulator is also lobbying the competent authorities to set up online public communication services enabling persons with disabilities to access the services of government administration, the local authorities and public establishments. The development of accessible technologies (haptic, remote control, voice announcements in public transportation, sound signals at pedestrian crossings, etc.) represents major progress for persons with disabilities, in particular the visually impaired and the blind. The Secretariat of State for Persons with has been authorized to plan training a cohort of 50 young persons with disabilities under its RepareNet programme, which aims to teach the young people how to repair their own defective phones and those of others, thereby enabling them to earn a significant income and to be part of the digital economy.

Mexico

In Mexico, IFT has introduced a complaint map to give users more insight into the record of each service provider as regards complaints, and the consensus in each region. Users of digital services are also able to use an interactive application to research and compare relevant characteristics of the policies and the terms and conditions used by the main digital platforms, terminal equipment vendors, and operating systems. It highlights the information that the user population shares with them and how that is manged, as well as the scope of the permissions that are granted when using these platforms.

For the development of the tool, information was identified and analysed for different digital platforms, terminal equipment vendors and operating systems and their policies, terms and conditions, and so on. The information that is integrated into the tool is related to the constantly evolving information provided by these companies. In this way users can keep up to date regarding their rights.

Office of the Director
International Telecommunication Union (ITU)
Telecommunication Development Bureau (BDT)
Place des Nations
CH-1211 Geneva 20
Switzerland

Email: bdtdirector@itu.int
Tel.: +41 22 730 5035/5435
Fax: +41 22 730 5484

Office of Deputy Director and Regional Presence
Field Operations Coordination Department (DDR)
Place des Nations
CH-1211 Geneva 20
Switzerland

Email: bdtdeputydir@itu.int
Tel.: +41 22 730 5131
Fax: +41 22 730 5484

Digital Networks and Society (DNS)
Email: bdt-dns@itu.int
Tel.: +41 22 730 5421
Fax: +41 22 730 5484

Digital Knowledge Hub Department (DKH)
Email: bdt-dkh@itu.int
Tel.: +41 22 730 5900
Fax: +41 22 730 5484

Partnerships for Digital Development Department (PDD)
Email: bdt-pdd@itu.int
Tel.: +41 22 730 5447
Fax: +41 22 730 5484

Africa

Ethiopia
International Telecommunication Union (ITU) Regional Office
Gambia Road
Leghar Ethio Telecom Bldg. 3rd floor
P.O. Box 60 005
Addis Ababa
Ethiopia

Email: itu-ro-africa@itu.int
Tel.: +251 11 551 4977
Tel.: +251 11 551 4855
Tel.: +251 11 551 8328
Fax: +251 11 551 7299

Cameroon
Union internationale des télécommunications (UIT)
Bureau de zone
Immeuble CAMPOST, 3e étage
Boulevard du 20 mai
Boîte postale 11017
Yaoundé
Cameroon

Email: itu-yaounde@itu.int
Tel.: + 237 22 22 9292
Tel.: + 237 22 22 9291
Fax: + 237 22 22 9297

Senegal
Union internationale des télécommunications (UIT)
Bureau de zone
8, Route du Méridien Président
Immeuble Rokhaya, 3e étage
Boîte postale 29471
Dakar - Yoff
Senegal

Email: itu-dakar@itu.int
Tel.: +221 33 859 7010
Tel.: +221 33 859 7021
Fax: +221 33 868 6386

Zimbabwe
International Telecommunication Union (ITU) Area Office
USAF POTRAZ Building
877 Endeavour Crescent
Mount Pleasant Business Park
Harare
Zimbabwe

Email: itu-harare@itu.int
Tel.: +263 242 369015
Tel.: +263 242 369016

Americas

Brazil
União Internacional de Telecomunicações (UIT)
Escritório Regional
SAUS Quadra 6 Ed. Luis Eduardo Magalhães,
Bloco "E", 10º andar, Ala Sul (Anatel)
CEP 70070-940 Brasilia - DF
Brazil

Email: itubrasilia@itu.int
Tel.: +55 61 2312 2730-1
Tel.: +55 61 2312 2733-5
Fax: +55 61 2312 2738

Barbados
International Telecommunication Union (ITU) Area Office
United Nations House
Marine Gardens
Hastings, Christ Church
P.O. Box 1047
Bridgetown
Barbados

Email: itubridgetown@itu.int
Tel.: +1 246 431 0343
Fax: +1 246 437 7403

Chile
Unión Internacional de Telecomunicaciones (UIT)
Oficina de Representación de Área
Merced 753, Piso 4
Santiago de Chile
Chile

Email: itusantiago@itu.int
Tel.: +56 2 632 6134/6147
Fax: +56 2 632 6154

Honduras
Unión Internacional de Telecomunicaciones (UIT)
Oficina de Representación de Área
Colonia Altos de Miramontes
Calle principal, Edificio No. 1583
Frente a Santos y Cía
Apartado Postal 976
Tegucigalpa
Honduras

Email: itutegucigalpa@itu.int
Tel.: +504 2235 5470
Fax: +504 2235 5471

Arab States

Egypt
International Telecommunication Union (ITU) Regional Office
Smart Village, Building B 147,
3rd floor
Km 28 Cairo
Alexandria Desert Road
Giza Governorate
Cairo
Egypt

Email: itu-ro-arabstates@itu.int
Tel.: +202 3537 1777
Fax: +202 3537 1888

Asia-Pacific

Thailand
International Telecommunication Union (ITU) Regional Office
4th floor NBTC Region 1 Building
101 Chaengwattana Road
Laksi,
Bangkok 10210,
Thailand

Email: itu-ro-asiapacific@itu.int
Tel.: +66 2 574 9326 – 8
+66 2 575 0055

Indonesia
International Telecommunication Union (ITU) Area Office
Gedung Sapta Pesona
13th floor
Jl. Merdeka Barat No. 17
Jakarta 10110
Indonesia

Email: bdt-ao-jakarta@itu.int
Tel.: +62 21 380 2322

India
International Telecommunication Union (ITU) Area Office and Innovation Centre
C-DOT Campus
Mandi Road
Chhatarpur, Mehrauli
New Delhi 110030
India

Email:
Area Office: itu-ao-southasia@itu.int
Innovation Centre: itu-ic-southasia@itu.int
Website: ITU Innovation Centre in New Delhi, India

CIS

Russian Federation
International Telecommunication Union (ITU) Regional Office
4, Building 1
Sergiy Radonezhsky Str.
Moscow 105120
Russian Federation
Email: itu-ro-cis@itu.int
Tel.: +7 495 926 6070

Europe

Switzerland
International Telecommunication Union (ITU) Office for Europe
Place des Nations
CH-1211 Geneva 20
Switzerland

Email: eurregion@itu.int
Tel.: +41 22 730 5467
Fax: +41 22 730 5484

International Telecommunication Union
Telecommunication Development Bureau
Place des Nations
CH-1211 Geneva 20
Switzerland

ISBN 978-92-61-40931-9

Published in Switzerland
Geneva, 2025

Photo credits: Adobe Stock