SECURING *the* FUTURE

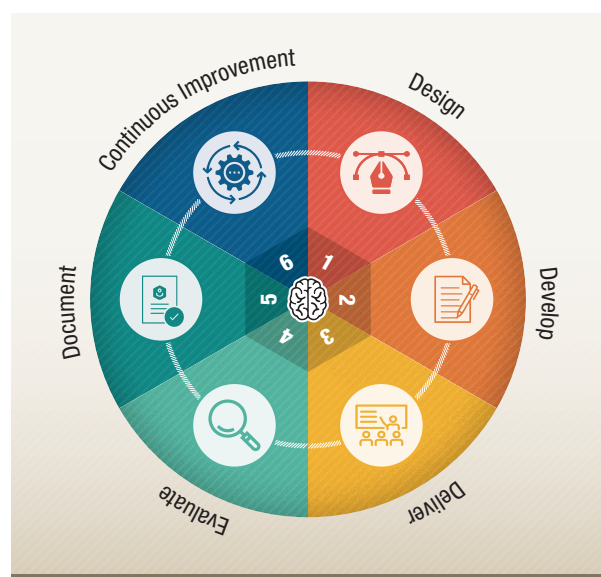## Child Online Protection Action Plan

By **Racky Seye**
Head of the Office of Information Systems Security and Digital Trust,
Senegal Ministry of Digital Economy and Telecommunications

Children and young people are among the most fervent users of mobile technologies. While this can have a positive impact on their education and lives, mobile technologies can also be harmful. Protecting children in cyberspace is as essential as it is in the physical world. Parents, governments and businesses have important roles to play in protecting and supporting connected children and helping them avoid deviant behavior and its detrimental consequences. To address this problem, it was crucial for Senegal to develop a national-level child online protection (COP) workforce and to conduct an action plan.
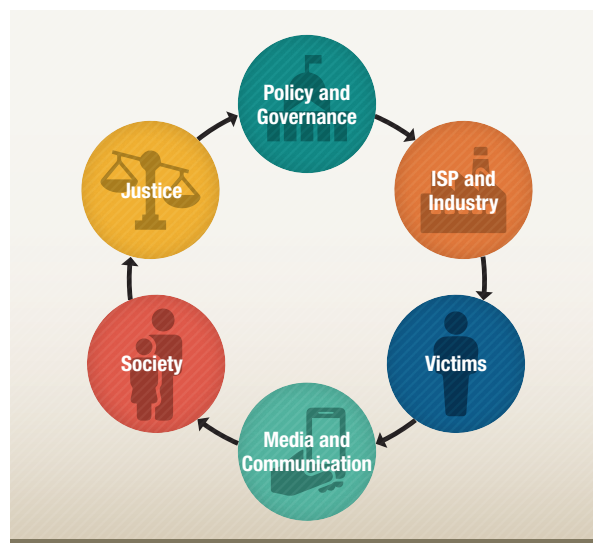
CHILD ONLINE PROTECTION PLAN

The penetration rate of internet services in Senegal is estimated at 68%. With 10.4 million internet subscribers, 41% of whom are under 15 years old, the government has made COP a priority, counting on the convergence and synergy of initiatives and the strengths of institutions, as well as on families and civic associations.

In this context, the government of Senegal has approved the Senegalese National Cybersecurity Strategy in accordance with the implementation of the Digital Senegal 2025 Strategy. This document aims to establish "a cyberspace of trust, secure and resilience for all" in Senegal by 2022 and also promote a generalized culture of cyber security. It highlights a specific objective: "Raising awareness of all the groups concerned as well as the general public on the security risks in cyberspace."

The National COP Action Plan follows from the implementation of this strategic objective. This plan, which demonstrates the commitment of Senegal to protecting children on the internet, rests on six pillars:

1. Policy and governance
2. Justice
3. Society
4. Media and communication
5. Victims
6. Internet service providers (ISP) and industry

THE SIX PILLARS

Each pillar includes activities — such as awareness-raising and training for children, parents and stakeholders — as well as setting up technical systems to better care for victims to ensure a balance between protecting children in the digital world and empowering them through the use of mobile and information and communications technology (ICT).

Within the implementation of this plan, in particular Pillar 1 concerning policy and governance, a steering committee of key players in COP from the public and private sectors and civil society was created through ministerial decree. It is chaired by the ICT directorate of the ministry in charge of the digital economy. Its objective is to lead the process of implementing the action plan through regular meetings and seminars.

At the start of each year, the committee uses the action plan to draw up an annual work plan that outlines activities for the year. This committee also serves as an international point of contact on matters relating to protecting children online.

Children and young people are the next generation of cyber-aware leaders, and national programs must address their unique needs now and society's comprehensive risks in the future. Whole-of-government approaches have proven effective. To create the next generation of the cyber workforce, such plans need to be brought to the fore of the cyber policy discussion. □