Resumo executivo

Dados Pessoais, poder institucional e apropriação cidadã: rumo a uma cultura de proteção de dados no Equador

Objetivo e alcance

Este relatório oferece um panorama abrangente do ecossistema de proteção de dados pessoais no Equador: combina uma análise do marco normativo e institucional com evidências qualitativas coletadas em grupos focais com duas populações particularmente expostas a riscos — pessoas LGBTIQ+ e comunidades amazônicas — para traduzir experiências reais em recomendações de política pública e ferramentas cidadãs.

Metodologia

O estudo triangula (i) uma revisão documental do marco vigente e de planos nacionais, com (ii) dois grupos focais independentes, realizados virtualmente, com consentimento informado, confidencialidade e protocolos para evitar revitimização. As dinâmicas incluíram mapas mentais, brainstorming e priorização coletiva guiada por quatro eixos: conhecimento e contexto; experiências e riscos; expectativas institucionais; e soluções necessárias. Os grupos foram compostos por ativistas e comunicadores LGBTIQ+, bem como líderes e defensores de povos amazônicos.

Contexto normativo e institucional

O Equador conta com um arcabouço legal atualizado (Constituição, Lei de Proteção de Dados Pessoais e legislação secundária) e uma agenda nacional que, se bem implementado sob responsabilidade proativa e privacidade desde a concepção, podem reduzir a lacuna entre o direito formal e sua garantia efetiva. O Plano Nacional de Proteção de Dados Pessoais prevê eixos como governança digital, universalização do direito e criação de um Registro Nacional de Proteção de Dados para fortalecer a rastreabilidade e o controle. Para tratamentos de tratamento de alto risco, o uso de Avaliações de Impacto sobre a Proteção de Dados (AIPD) atua como evidência de conformidade e gestão de riscos.

Ao mesmo tempo, a Superintendência de Proteção de Dados Pessoais (SPDP) —autoridade nova — necessita de independência, orçamento adequado e capacidades técnicas para evoluir da “conformidade declarativa” à responsabilização demonstrável em todos os setores.

Principais conclusões

- **Lacunas de conhecimento e caminhos confusos:** A população tem pouco conhecimento da LOPDP, dos direitos ARCO e de como funciona o Sistema de Proteção de Dados (funções do controlador/operador de dados, DPO, competências da SPDP), o que desencoraja a ativação de mecanismos formais e normaliza práticas inadequadas.
- **Práticas problemáticas recorrentes:** São relatados casos de telemarketing com bases de dados compradas, reutilização de formulários, pedidos injustificados de dados sensíveis e perda de controle em plataformas. Esses padrões aumentam os riscos de discriminação, fraude, insegurança digital e criminalização de defensores.
- **Desconfiança institucional:** A distância entre os avanços normativos e sua aplicação cotidiana alimenta a percepção de ineficácia e limita o exercício de direitos.

- **Reconhecimento de dados coletivos:** Nos territórios amazônicos, enfatiza-se a necessidade de proteger dados coletivos e culturais, com salvaguardas adequadas ao contexto, idioma e cosmovisões.

Recomendações estratégicas

1. **Responsabilidade proativa e privacidade desde a concepção:** Promover metodologias de gestão de riscos e EIPD ao longo de todo o ciclo de vida dos dados; incentivar códigos de conduta/certificações; e assegurar a minimização e a transparência como princípios orientadores.
2. **Fortalecimento dos principais atores:** Reforçar o papel do Encarregado de Proteção de Dados (DPO) em entidades públicas e privadas; e dotar o SSPD de independência, orçamento e equipes técnicas para avaliar impactos, mitigações e riscos residuais.
3. **Transparência e controle cidadão efetivos:** Exigir avisos de privacidade compreensíveis, painéis de controle para gestão do consentimento, rastreabilidade das fontes e canais de reclamação acessíveis; avançar na criação de um Registro Nacional de Proteção de Dados que facilite a supervisão e auditoria social.
4. **Enfoque diferencial e territorial:** Reconhecer e proteger os dados coletivos em comunidades amazônicas; adaptar políticas e serviços para superar barreiras de idioma, cultura, discriminação e conectividade.
5. **Educação prática e multicanal:** Desenvolver campanhas segmentadas por idade e região, com materiais em múltiplos formatos (áudio-radiais, infográficos, cartilhas bilíngues, conteúdo para redes sociais) e conteúdos práticos: como denunciar, configurar 2FA, reconhecer phishing, exercer o direito de revogação. Incluir rotas offline em áreas de baixa conectividade.

Conclusão

O país já dispõe de bases jurídicas e uma agenda nacional para proteger dados pessoais; o desafio está em traduzi-las em capacidades, processos e cultura pública e organizacional. Com responsabilidade proativa, transparência aplicável e educação prática — especialmente em populações historicamente vulnerabilizadas — é possível fechar a lacuna entre a promessa legal e a garantia efetiva do direito à proteção de dados no Equador.