

Inclusion numérique et atteintes à la vie privée en Équateur : une analyse socio-historique des technologies de la communication

Digital Inclusion and Privacy Violations in Ecuador: A Socio-Historical Analysis of Communication Technologies

*Inclusión digital y vulneración de la privacidad en Ecuador:
un análisis socio-histórico de las tecnologías de la comunicación*

Barcos-Arias, Ignacio F.

Universidad Regional Autónoma de los Andes, Sede Babahoyo, Équateur

ub.ignaciobarcos@uniandes.edu.ec

 <https://orcid.org/0000-0002-9493-7931>

Coello-Bustamante, Emily A.

Universidad Regional Autónoma de los Andes, Sede Babahoyo, Équateur

db.emilyacb35@uniandes.edu.ec

 <https://orcid.org/0000-0001-7177-0668>

Résumé

Cet article analyse, dans une perspective socio-historique, les technologies de la communication en Équateur et leur impact sur le droit à la vie privée. Son objectif est d'examiner comment l'expansion de la connectivité numérique a simultanément favorisé l'inclusion sociale et intensifié les mécanismes d'extraction de données, les atteintes à la vie privée et les asymétries de protection des droits. Sur le plan

méthodologique, l'étude combine une analyse narrative, normative et socio-historique de l'expansion numérique en Équateur avec l'examen de cas emblématiques tels que Novaestrat, les logiciels espions régionaux et les dispositifs de traçage déployés pendant la pandémie. Les résultats montrent que l'essor de la connectivité s'est accompagné d'une intensification de l'extraction de données, de larges exceptions juridiques, de capacités institutionnelles limitées et de fortes inégalités territoriales et sociales dans la protection effective des droits. L'article conclut que l'inclusion numérique en Équateur est traversée par des tensions structurelles entre innovation technologique, surveillance, inégalités et souveraineté informationnelle, ce qui exige des réformes normatives, institutionnelles et éducatives capables de rendre effectifs les droits dans l'environnement numérique.

Mots-clés : inclusion numérique, vie privée, protection des données, souveraineté informationnelle, Équateur.

Abstract

This article analyzes communication technologies in Ecuador and their impact on privacy rights from a socio-historical perspective. Its objective is to examine how the expansion of digital connectivity has simultaneously fostered social inclusion and intensified data extraction, privacy violations, and asymmetries in rights protection. Methodologically, the study combines a narrative, normative, and socio-historical analysis of digital expansion in Ecuador with the examination of emblematic cases such as Novaestrat, regional spyware practices, and pandemic-era tracking mechanisms. The findings show that expanding connectivity has been accompanied by intensified data extraction, broad legal exceptions, limited institutional capacity, and strong territorial and social inequalities in the effective protection of rights. The article concludes

that digital inclusion in Ecuador is marked by structural tensions among technological innovation, surveillance, inequality, and informational sovereignty, thus requiring legal, institutional, and educational reforms capable of making rights enforceable in digital environments.

Keywords: digital inclusion, privacy, data protection, informational sovereignty, Ecuador.

Resumen

Este artículo analiza las tecnologías de la comunicación en Ecuador y su impacto en el derecho a la privacidad desde una perspectiva socio-histórica. Su objetivo es examinar cómo la expansión de la conectividad digital ha favorecido simultáneamente la inclusión social y la intensificación de la extracción de datos, las vulneraciones de la privacidad y las asimetrías en la protección de derechos. Metodológicamente, el estudio combina un análisis narrativo, normativo y socio-histórico de la expansión digital en Ecuador con el examen de casos emblemáticos como Novaestrat, las prácticas regionales de software espía y los mecanismos de rastreo implementados durante la pandemia. Los resultados muestran que el crecimiento de la conectividad ha venido acompañado de una intensificación de la extracción de datos, amplias excepciones legales, capacidades institucionales limitadas y fuertes desigualdades territoriales y sociales en la protección efectiva de derechos. Se concluye que la inclusión digital en Ecuador está atravesada por tensiones estructurales entre innovación tecnológica, vigilancia, desigualdad y soberanía informativa, lo que exige reformas normativas, institucionales y educativas capaces de hacer exigibles los derechos en los entornos digitales.

Palabras clave: inclusión digital, privacidad, protección de datos, soberanía informativa, Ecuador.

Reçu : 4 juin 2026 - **Accepté :** 10 septembre 2026

1. Introduction

Dans la seconde moitié du XXe siècle, les technologies de la communication ont promis d'abolir les distances, de démocratiser le savoir et de favoriser un réseau mondial de solidarité. Des premières liaisons satellitaires en Amérique latine à l'arrivée d'Internet dans les années 1990, à l'essor de la téléphonie mobile dans les années 2000, puis à l'implantation massive des réseaux sociaux et de l'intelligence artificielle dans les années 2010, ces technologies ont été présentées comme des vecteurs d'inclusion sociale, d'autonomisation citoyenne et de croissance économique. En Équateur, ce narratif semble se confirmer : en 2000, seuls 2 % de la population avaient accès à Internet ; au début des années 2020, ce chiffre dépassait 70 % (INEC, 2023), avec une adoption particulièrement élevée dans les zones urbaines par rapport aux zones rurales. La pandémie de 2020 a accéléré l'adoption du numérique : l'enseignement virtuel, le télétravail et les achats en ligne sont devenus essentiels, tandis que WhatsApp, Facebook, TikTok et

Instagram se sont imposés comme des infrastructures centrales de la participation sociale et économique.

Sous ce « miracle » de l'hyperconnectivité se dessine toutefois une nouvelle frontière d'exclusion et de violations de droits : les atteintes systématiques à la vie privée. Ce qui apparaît comme un accès libre et démocratique constitue, en réalité, un système continu d'extraction de données qui transforme les usagers en unités au sein d'un vaste réservoir informationnel contrôlé par des entreprises technologiques multinationales, des gouvernements et des algorithmes opaques. Cette dynamique peut également être comprise à travers des disjonctions transnationales plus larges entre l'expansion des infrastructures numériques transfrontalières et la protection institutionnelle inégale dont disposent des sujets dont les droits demeurent territorialement fragmentés (Parella y Speroni, 2018). En Amérique latine, où plus de 40 % de la population rurale ne disposait pas d'un accès stable en 2025 (CEPAL, 2023), la promesse de l'inclusion numérique tend

souvent à renforcer les inégalités existantes – de classe, de genre, d’ethnicité et de territoire – tandis que les atteintes à la vie privée deviennent un coût politisé du progrès.

La compréhension historique est essentielle. L’accès à Internet en Équateur a débuté dans les années 1990, et fut d’abord limité aux universités et aux élites urbaines – le premier nœud ayant été installé à l’ESPOL en 1992 – avant de s’étendre après la libéralisation des télécommunications (Loi sur les télécommunications de 1992 ; Loi réformée sur les télécommunications de 2002). La reconnaissance constitutionnelle de la vie privée a émergé avec la *Constitución del Ecuador* de 2008 (article 66, paragraphe 20), mais sa mise en œuvre est restée en retard par rapport à l’expansion numérique. La *Ley Orgánica de Protección de Datos Personales* (LOPDP, 2021) s’aligne sur les standards internationaux (RGPD et OEA), mais son application demeure limitée : la Superintendencia de Protección de Datos Personales (SPDP) fait face à des contraintes budgétaires et de personnel, et les sanctions

pour les violations massives restent presque inexistantes.

Entre 2020 et 2022, le confinement a accéléré la numérisation, générant une collecte massive de données (localisation, contacts, santé, consommation), souvent sans consentement éclairé. Des applications telles que *Plan Vacunarse* et les plateformes d’enseignement à distance ont exigé des données sensibles de millions de personnes, tandis que les réseaux sociaux sont devenus essentiels pour l’accès aux services gouvernementaux ou commerciaux. Ces mesures ont aggravé l’exclusion numérique et facilité la surveillance algorithmique comme forme de contrôle social.

La littérature académique latino-américaine sur ce sujet demeure encore embryonnaire et fragmentée. Tandis que les études internationales (Zuboff, 2019 ; Lyon, 2018) abordent le « capitalisme de surveillance » et les « sociétés de contrôle » (Deleuze, 1990), les travaux latino-américains privilégient souvent des perspectives techniques ou juridiques

(LOPDP, RGPD), peu d'entre eux intégrant une analyse historique ou critique. Il existe peu de recherches retraçant une narration chronologique allant de la télégraphie à l'intelligence artificielle, montrant comment les technologies incorporent des héritages coloniaux et patriarcaux et transforment des populations vulnérables en réservoirs de données faiblement protégés. Cette lacune historiographique est particulièrement visible en Équateur, où l'avancement technologique est souvent célébré sans examen critique de ses implications pour la vie privée et l'autonomie.

Cette étude entend combler cette lacune à travers une analyse socio-historique des technologies de la communication en Équateur et de leur impact sur le droit à la vie privée. Elle vise à examiner comment l'expansion de la connectivité numérique a simultanément favorisé l'inclusion sociale et intensifié les mécanismes d'extraction de données, les atteintes à la vie privée et les asymétries dans la protection effective des droits. À partir de ce constat, l'article

analyse l'évolution constitutionnelle et juridique de la protection des données, identifie les principales violations liées aux usages étatiques et commerciaux des technologies numériques, et met en évidence leurs conséquences en termes d'exclusion numérique, de vulnérabilité différenciée et de souveraineté informationnelle en Équateur et en Amérique latine.

En définitive, cette approche suggère que la « connectivité mondiale » n'est pas un miracle neutre, mais une frontière de pouvoir, d'exclusion et de résistance. Les inégalités historiques, combinées aux fractures numériques, font des atteintes à la vie privée non pas des phénomènes accidentels, mais des éléments constitutifs des régimes contemporains de *big data*.

2. La « rébellion » numérique comme autorisation de l'extraction des données

Le phénomène socio-économique à travers lequel les technologies de la communication auraient démocratisé l'Amérique latine au

cours des trente dernières années n'a pas constitué un processus neutre et linéaire de modernisation technologique. En adoptant massivement les dispositifs et les plateformes numériques dans un cadre normatif de liberté, de connexion et de développement, les usagers ont, souvent sans en avoir pleinement conscience, contribué à rendre possible l'expropriation massive des données personnelles. Cette « rébellion » ne renvoie donc pas à un renversement du pouvoir par les dominés, mais à une dynamique dans laquelle le capital technologique et les appareils étatiques étendent leur emprise sur la souveraineté informationnelle des individus. L'Équateur ne fait pas exception à cette dynamique, compte tenu du décalage juridique et empirique observable dans le pays.

D'un point de vue constitutionnel, l'écart entre la protection juridique formelle – inscrite dans la *Constitución del Ecuador* de 2008, notamment à l'article 66, paragraphe 20 – et son application concrète – à travers la LOPDP de 2021 et

les rapports institutionnels récents de la Superintendencia de Protección de Datos Personales (SPDP) – révèle l'existence de larges exceptions qui tendent moins à protéger les données personnelles qu'à encadrer de manière ambiguë leur exploitation. Ces dynamiques traversent l'ensemble du pays, du Pacifique à l'Amazonie, facilitées à la fois par les intérêts des entreprises et par les marges d'exception reconnues à l'État, ce qui entretient un décalage notable entre les promesses constitutionnelles et la réalité effective de la protection des données.

2.1. De la Constitución del Ecuador de 2008 à la Ley Orgánica de Protección de Datos Personales de 2021 : chronologie de la promesse normative face à la réalité des exceptions

La *Constitución de la República del Ecuador* de 2008 constitue le premier texte constitutionnel équatorien à reconnaître explicitement, dans un cadre juridiquement défini, la nécessité de protéger les données. Elle inscrit ce droit dans le champ plus large de la vie privée et de l'autodétermination informationnelle. L'article 66, paragraphe

20, établit que toute personne a droit « à la protection de ses données personnelles, de sa vie privée et familiale, ainsi que de son honneur et de sa réputation ». Bien qu'inspirée par des tendances régionales – notamment la Constitution colombienne de 1991 et la Constitution bolivienne de 2009 – ainsi que par la numérisation croissante de la société, cette disposition est restée vague et, pendant plus d'une décennie, dépourvue d'une autorité de contrôle effective ou d'une loi spécifique d'application.

Entre 2008 et 2015, cet écart d'application a favorisé l'essor de collectes de données sans consentement éclairé. Les entreprises de télécommunications (CNT, Claro, Movistar) ont accumulé des métadonnées – localisation, contacts, habitudes de consommation – sous couvert d'une « amélioration des services », tandis que les grandes plateformes mondiales (Facebook, Google, WhatsApp) faisaient de même. Dans le même temps, les initiatives étatiques ont cherché à numériser les systèmes de sécurité, notamment à travers le *Servicio Integrado de Seguridad ECU 911*, mis

en place en 2014 et fondé sur des réseaux de caméras, la reconnaissance faciale et des bases de données. Pendant la pandémie de 2020, des plateformes numériques à vocation inclusive telles que *Plan Vacunarse* et les systèmes obligatoires de traçage des contacts ont exposé des données personnelles sensibles sans mécanismes adéquats de protection ni de reddition de comptes.

La LOPDP a été promulguée le 26 mai 2021 et est entrée en vigueur en mai 2022. Bien qu'elle ait été élaborée sur le modèle du RGPD européen, sa mise en œuvre pratique est restée en décalage avec la réalité numérique. La loi établit des principes de légalité, de transparence, de limitation de finalité, de minimisation des données, d'intégrité et de confidentialité. Les articles 11 à 19 définissent les exigences de consentement pour le transfert international de données ainsi que pour les catégories sensibles de données, notamment la santé, l'ethnicité et l'orientation sexuelle. Toutefois, l'article 4 prévoit des exceptions pour la sécurité nationale, l'intérêt public ou les urgences

sanitaires, contournant de fait l'exigence de consentement.

Ces catégories imprécises ont favorisé le développement de formes de surveillance de masse et de bases de données centralisées. Prévues par la LOPDP de 2021, mais dont le premier superintendant n'a été désigné qu'en 2024, la SPDP possède une capacité d'application limitée. Les sanctions imposées en cas de violations à grande échelle demeurent négligeables au regard de l'ampleur des atteintes. À titre d'exemple, l'affaire *Novaestrat* a exposé les données de plus de vingt millions d'Équatoriens en 2019, alors que les sanctions appliquées n'ont concerné qu'une part mineure du dommage. Les entreprises technologiques transnationales continuent, par ailleurs, d'opérer au moyen de clauses de consentement opaques, en transférant des données à l'intérieur et à l'extérieur du pays sous une supervision minimale. Ainsi, si la LOPDP représente une promesse normative, sa mise en œuvre pratique demeure incohérente et arbitraire, faisant

de l'extraction massive de données une pratique structurelle et ordinaire.

2.2. Du Pacifique à l'Amazonie et inversement : transferts régionaux de vulnérabilité

La réalité équatorienne n'existe pas en vase clos : elle s'inscrit dans des circulations transfrontalières qui vont du Pacifique à l'Amazonie. En Colombie, la surveillance étatique s'est intensifiée avec la mise en œuvre du système d'information sur la sécurité et la défense (SISD) et avec l'usage de *Pegasus*, signalé par *Citizen Lab* entre 2021 et 2023. Des initiatives de grande ampleur, comme le projet de registre national de 2018 portant sur les données de quarante millions de citoyens, révèlent à la fois les failles réglementaires et la faiblesse de la responsabilité étatique et des entreprises.

Au Pérou, l'adoption de la *Ley n°29733 de Protección de Datos Personales* (2011) fut antérieure à la LOPDP équatorienne, mais son application demeure limitée. Les applications de livraison et de transport, telles que *Rappi* et *Cabify*, exploitent commercialement les

données des usagers avec une régulation minimale. Dans certaines régions, les populations autochtones amazoniennes font également l'objet de dispositifs de surveillance liés à des enquêtes de la *Comisión Nacional para el Desarrollo y Vida sin Drogas* (DEVIDA).

Au Chili, la *Ley* n° 19.628, actualisée en 2023, ainsi que la création de l'*Agencia de Protección de Datos Personales* en 2024, témoignent d'un potentiel institutionnel plus élevé. Néanmoins, des lacunes importantes subsistent : la fuite de données des *Carabineros* en 2022 a affecté plus de dix millions de personnes, et la reconnaissance faciale a été utilisée pour surveiller les manifestations socio-politiques entre 2019 et 2022, souvent au nom de la sécurité nationale.

Les flux régionaux de données transitent par des plateformes comme *Meta*, *Google* et *TikTok*. Des outils gouvernementaux comme *Pegasus* et *Candiru* fonctionnent également à travers les frontières. Des violations historiques, telles que *Novaestrat* (2019), ont influencé les débats publics au Pérou et en Colombie,

illustrant la dimension transfrontalière de la vulnérabilité numérique.

Les transferts transfrontaliers de données dans les territoires amazoniens et frontaliers aggravent encore ces risques. Les populations urbaines et rurales sont affectées de manière différenciée à travers des registres tels que le SINAD et le RUPC, dans un contexte de faible littératie numérique et de mesures de protection négligeables. Dans ces conditions, l'inclusion devient un vecteur de dépendance informationnelle et d'asymétrie numérique : les populations connectées du Pacifique interagissent avec les communautés amazoniennes à travers des fractures numériques extrêmes. Cette « rébellion » numérique structurelle accorde un accès à la connectivité dans des conditions qui sacrifient systématiquement la vie privée.

3. Transferts frontaliers et circulations de l'intimité numérique

L'essor des technologies de la communication ne s'est pas limité à un développement

strictement national ; il s'inscrit dans un processus transnational et transfrontalier de transferts et d'échanges qui relie le continent latino-américain, du Pacifique à l'Amazonie, et des centres urbains aux périphéries rurales et autochtones. Il s'agit d'un processus à la fois technique – codes, protocoles, algorithmes – et profondément politique et économique. Les données personnelles circulent à travers des infrastructures globales avec un contrôle limité, tandis que les atteintes à la vie privée affectent de manière disproportionnée les populations vulnérables. En Équateur comme dans le reste de l'Amérique latine, la vie privée numérique peut ainsi être comprise comme une frontière poreuse et asymétrique : les usagers fournissent des informations en échange d'accès et de services, tandis que des acteurs technologiques, étatiques et criminels collectent, stockent et exploitent ces données avec des conséquences juridiques limitées. Cette section présente des cas emblématiques, met en évidence les formes d'atteinte à la vie privée et analyse les barrières structurelles qui transforment la fracture numérique en multiplicateur d'exclusion.

3.1. Cas emblématiques de fuites de données et de surveillance de masse

L'affaire Novaestrat (2019) constitue l'une des violations de données les plus significatives en Équateur. Un serveur non sécurisé a exposé des informations concernant plus de vingt millions de personnes, notamment des noms, numéros d'identification nationale, adresses, numéros de téléphone, courriels et autres données sociodémographiques. Au moment de la fuite, la LOPDP n'était pas encore entrée en vigueur – son application effective ne date que de 2021-2022 – et l'ampleur de l'incident a mis en évidence l'absence de mécanismes efficaces de supervision ainsi que de garanties institutionnelles capables de prévenir ou de contenir rapidement des expositions de cette ampleur.

Après la mise en place de la SPDP en 2024, des procédures d'enquête ont été engagées. Toutefois, les capacités de mise en œuvre sont demeurées limitées en termes de ressources humaines, de budget et de portée des sanctions. Dans les cas de grande ampleur, les sanctions n'ont pas nécessairement donné

lieu à des réparations complètes pour les personnes affectées. L'affaire *Novaestrat* a également eu une résonance régionale et peut être comparée à d'autres expositions massives de données dans la région andine, telles que l'incident du RENIEC au Pérou en 2019 et la fuite du *Registro Nacional* en Colombie en 2018, chacun concernant des dizaines de millions d'enregistrements.

Le scandale *Cambridge Analytica* (2018) a, en outre, démontré le caractère transnational de l'exploitation des données en Amérique latine. Cette société de conseil britannique a recueilli les données d'utilisateurs de Facebook afin d'influencer des campagnes électorales, notamment au Brésil et en Colombie. Des rapports d'enquête ont indiqué que des profils provenant de plusieurs pays latino-américains, dont l'Équateur et le Pérou, avaient été indirectement affectés par des flux transfrontaliers de données. Ce cas illustre la manière dont des données collectées localement peuvent être traitées, analysées et mobilisées à l'échelle internationale, souvent au-delà

de la juridiction effective des cadres réglementaires nationaux.

Les mécanismes de surveillance étatique ont ajouté un niveau supplémentaire de complexité. Le *Servicio Integrado de Seguridad ECU 911* a incorporé des technologies de surveillance, y compris des outils de reconnaissance faciale, dans le cadre du système de sécurité publique équatorien, encadré notamment par la *Ley de Seguridad Pública y del Estado* de 2009. En outre, l'article 4 de la LOPDP prévoit des exceptions pour la sécurité nationale et l'intérêt public, ce qui peut autoriser une extension du traitement des données sans consentement individuel. Des rapports de *Citizen Lab* (2021–2023) ont documenté l'utilisation de logiciels espions tels que *Pegasus* dans plusieurs pays de la région, avec des cas confirmés dans certains contextes nationaux et des préoccupations quant à leur possible extension à d'autres pays.

Dans un contexte régional élargi, l'usage de technologies de reconnaissance faciale lors des manifestations publiques au Chili

(2019–2022), ainsi que les pratiques de surveillance affectant les populations autochtones amazoniennes au Pérou et en Colombie ont soulevé des préoccupations d'ordre constitutionnel et liées aux droits humains. Ces exemples montrent comment les pratiques de surveillance numérique peuvent affecter de manière disproportionnée des groupes politiquement actifs et territorialement marginalisés.

Les plateformes privées jouent également un rôle central. Des applications telles que *WhatsApp* – propriété de Meta Platforms – et largement utilisées en Équateur, avec des taux de pénétration dépassant 80 % parmi les internautes, collectent des métadonnées liées aux communications et à la localisation dans le cadre de régimes de consentement contractuel. Les transferts de données vers des serveurs situés à l'étranger, fréquemment justifiés comme des « transferts internationaux » en vertu de la législation nationale, soulèvent des questions quant à l'auditabilité et à l'effectivité de la supervision réglementaire.

Pris ensemble, ces cas révèlent que la vie privée numérique en Équateur et dans la région andine est façonnée par une combinaison d'extraction corporative de données, de pratiques de surveillance étatique, de flux transfrontaliers de données et de capacités institutionnelles limitées en matière de contrôle et de sanction. Afin de systématiser les cas présentés ci-dessus et de les situer dans une perspective à la fois chronologique et régionale, le Tableau 1 propose une vue d'ensemble des violations emblématiques de la vie privée et des réponses normatives correspondantes en Équateur et dans certains pays latino-américains. Il met en évidence le décalage entre l'accélération technologique, les formes d'atteinte à la vie privée et les capacités institutionnelles de régulation.

Tableau 1. Chronologie des violations emblématiques et des réponses normatives en Équateur et en Amérique latine (sélection représentative)

Période	Principal cas / événement	Pays concernés	Type de violation	Réponse réglementaire / principal résultat
Avant 2010	Arrivée massive d’Internet et des premiers réseaux sociaux (MySpace, Facebook)	Équateur, Colombie, Pérou	Collecte initiale sans régulation	Absence de réglementation spécifique ; la Constitución del Ecuador de 2008 incorpore le droit à la vie privée (art. 66)
2010-2020	Essor des smartphones et des applications (WhatsApp 2010, TikTok 2016) ; fuite Novaestrat en 2019	Équateur, Pérou	Fuites massives, métadonnées commerciales	Loi péruvienne 29733 (2011) ; scandale Cambridge Analytica (2018) ; LOPDP équatorienne de 2021 (réaction tardive)
2020-2023	Pandémie de COVID-19 : applications de traçage des contacts, télétravail, éducation virtuelle ; usage de Pegasus	Équateur, Chili, Colombie	Surveillance massive liée à la santé et surveillance étatique	Exceptions pour « urgence sanitaire » dans la LOPDP ; rapports de Citizen Lab sur Pegasus en Amérique latine et dans les Caraïbes
2024-2026	IA générative, reconnaissance faciale au sein d’ECU 911 et nouvelles fuites mineures	Équateur, Chili	Surveillance algorithmique et commerciale continue	Sanctions symboliques de la SPDP ; réformes partielles de la LOPDP ; forte proportion de cas sans sanction effective

Source : élaboration propre à partir de rapports institutionnels récents de la SPDP, des investigations de Citizen Lab (2021-2023), des données de la CEPAL et des statistiques INEC-ENTIC (2023).

3.2. Architecture de l'impunité et réponse institutionnelle

La récurrence des violations massives de la vie privée en Équateur ne peut être expliquée uniquement par des défaillances techniques en matière de sécurité. Ces incidents révèlent plutôt une configuration structurelle dans laquelle la reconnaissance normative de la protection des données coexiste avec une capacité d'application limitée. Cette configuration peut être conceptualisée comme une « architecture de l'impunité », c'est-à-dire comme un écart systémique entre les garanties constitutionnelles et leur réalisation effective. Bien que la *Constitución del Ecuador* de 2008 ait consacré le droit à la protection des données personnelles, son application concrète dépend de la capacité institutionnelle, de la clarté réglementaire et de l'articulation judiciaire. Dans ce contexte, la LOPDP, promulguée en 2021, a représenté une avancée normative significative alignée sur des standards internationaux tels que le RGPD européen. Toutefois, la transition entre l'alignement normatif et l'efficacité opérationnelle s'est révélée inégale.

3.2.1 Limites pratiques de la Superintendencia de Protección de Datos Personales (SPDP)

La création de la Superintendencia de Protección de Datos Personales (SPDP) a constitué une étape institutionnelle importante dans le cadre réglementaire équatorien. Néanmoins, des contraintes structurelles ont affecté sa capacité de mise en œuvre. En 2025, la SPDP fonctionnait avec des ressources humaines limitées, chargées de superviser des activités de traitement de données affectant des millions d'utilisateurs et des milliers d'entités publiques et privées. Cette disproportion entre le mandat réglementaire et les ressources institutionnelles limite la supervision proactive et réduit la capacité de mener des audits systématiques.

Bien que la LOPDP établisse un régime administratif de sanctions, l'application concrète de celles-ci a soulevé des interrogations quant à leur proportionnalité et à leur effet dissuasif dans les cas de grande ampleur. Dans l'affaire Novaestrat, par exemple, des sanctions ont été appliquées dans le cadre

juridique existant. Néanmoins, leur portée n'a pas nécessairement correspondu à l'ampleur de la violation, ni permis de mettre en place des mécanismes complets de réparation pour les personnes affectées. Selon les rapports institutionnels publiés par la SPDP en 2025, une proportion significative des plaintes liées à la vie privée n'aboutit pas à des sanctions formelles. Qu'il s'agisse de charges probatoires élevées, de limitations procédurales, de complexité juridictionnelle ou d'absence de traçabilité technique suffisante, cette situation peut alimenter chez les citoyens une perception de protection réglementaire limitée.

Dans l'ensemble, ces éléments suggèrent que le régime équatorien de protection des données se caractérise non par l'absence de normes, mais par la fragilité de leur application. L'architecture de l'impunité relève donc moins d'une dérégulation explicite que d'une asymétrie structurelle entre des infrastructures numériques en expansion rapide et une consolidation institutionnelle comparativement lente.

3.2.2. « Exception normalisée » et surveillance algorithmique

Une dimension critique du cadre équatorien de protection des données réside dans la portée de l'article 4 de la LOPDP, qui prévoit des exceptions à l'exigence de consentement préalable dans les cas touchant à la sécurité nationale, à l'intérêt public ou à la santé publique. Bien que de telles exceptions ne soient pas inhabituelles dans la législation comparée, leur formulation large soulève des interrogations quant à la proportionnalité, à la nécessité et à l'existence de mécanismes effectifs de contrôle. Lorsque ces catégories sont interprétées de manière extensive, elles peuvent normaliser des pratiques extraordinaires de traitement des données et déplacer l'équilibre au détriment de l'autodétermination informationnelle des individus.

La pandémie de COVID-19 en fournit une illustration pertinente. Des outils numériques tels que *Plan Vacunarse* ont exigé le traitement de données sensibles relatives à la santé et à la mobilité de millions de citoyens dans le contexte d'une urgence sanitaire.

Bien que ces mesures aient été encadrées par une logique de gouvernance de crise, la gestion à long terme, le stockage et la suppression des données collectées n'ont pas été pleinement clarifiés dans des mécanismes d'audit publiquement accessibles. Cette situation met en lumière la tension entre le traitement des données fondé sur l'urgence et l'obligation de reddition de comptes après la fin de la crise.

De manière similaire, le développement des technologies biométriques au sein du *Servicio Integrado de Seguridad ECU 911* reflète l'incorporation croissante de la reconnaissance faciale et de l'analyse à grande échelle des métadonnées dans des logiques de sécurité publique. Bien que ces outils soient juridiquement justifiés dans des cadres liés à la sécurité nationale, leur déploiement soulève des préoccupations plus larges concernant la transparence algorithmique, l'usage proportionné et la supervision indépendante, en particulier dans des contextes où les capacités institutionnelles restent limitées.

Dans cette perspective, le concept d'« exception normalisée » ne renvoie pas à l'illégalité intrinsèque de ces mesures, mais au risque que des justifications exceptionnelles soient routinisées dans la gouvernance quotidienne. À mesure que les infrastructures numériques s'étendent, les individus évoluent de plus en plus au sein d'environnements où le traitement des données est intégré à l'accès aux services, à la mobilité et à la communication. En l'absence de garanties solides, d'exigences de transparence et d'une application effective du droit, cette asymétrie structurelle peut affaiblir les garanties concrètes de la vie privée et du respect de la procédure dans les contextes de prise de décision algorithmique.

3.2.3. Inégalité d'accès et « revictimisation numérique »

L'impunité numérique n'affecte pas tous les secteurs sociaux de manière égale. Plutôt que d'être distribués uniformément, les risques pesant sur la vie privée sont médiatisés par des inégalités structurelles qui façonnent la capacité des individus et

des communautés à comprendre, exercer et défendre leurs droits numériques. En ce sens, la fracture numérique n'opère pas seulement comme un écart de connectivité, mais aussi comme une exposition différenciée à la vulnérabilité.

Les enquêtes nationales disponibles indiquent qu'une proportion significative de la population ne dispose pas des compétences numériques avancées nécessaires pour exercer des droits tels que la rectification, la suppression ou l'opposition, conformément à l'article 12 de la LOPDP. Cette limitation n'implique pas une négation formelle des droits, mais plutôt une capacité inégale à les opérationnaliser en pratique, notamment chez les personnes âgées et les groupes à faibles revenus. Par conséquent, l'effectivité de la protection des données dépend non seulement de leur reconnaissance juridique, mais aussi des compétences numériques des citoyens.

Les études sur la violence numérique en Équateur et en Amérique latine montrent

également que les femmes et les personnes LGBTIQ+ sont exposées de manière disproportionnée au cyberharcèlement, au doxxing et à la diffusion non consentie d'informations personnelles. Les rapports disponibles indiquent que ces formes de violence s'inscrivent dans des contextes plus larges d'inégalités sociales et s'accompagnent souvent de faibles niveaux de signalement, de méfiance envers les institutions, de peur de la revictimisation et de l'absence de mécanismes de réponse suffisamment sensibles au genre (Defensoría del Pueblo del Ecuador, 2023 ; OEA y ONU Mujeres, 2022). Ces facteurs contribuent à une dynamique de « revictimisation numérique » dans laquelle les groupes affectés subissent à la fois une exposition accrue et une réparation institutionnelle limitée.

Des disparités importantes persistent enfin entre les zones urbaines et rurales en matière d'accès au haut débit et de connectivité stable, les ménages autochtones étant particulièrement affectés. Dans des contextes où l'accès est limité et la littératie numérique

inégale, les individus peuvent dépendre de systèmes numériques imposés par l'État ou par des plateformes sans comprendre pleinement les implications du traitement de leurs données. Cette asymétrie accroît la vulnérabilité tout en réduisant la capacité de supervision ou de résistance effective. Dans l'ensemble, les réponses institutionnelles à la vulnérabilité numérique en Équateur révèlent un écart entre les garanties normatives et les réalités sociales différenciées. Les données personnelles ont acquis une valeur économique et politique croissante, mais la capacité à exercer l'autodétermination informationnelle demeure inégalement distribuée, reproduisant ainsi des schémas préexistants d'exclusion sociale dans la sphère numérique.

3.3. Barrières structurelles : fracture numérique, stigmatisation et accès inégal

La vulnérabilité numérique en Équateur est distribuée de manière inégale et étroitement liée aux inégalités socio-économiques et territoriales préexistantes. La fracture numérique fonctionne comme un facteur

structurel qui conditionne à la fois l'accès à la connectivité et l'exercice effectif des droits en matière de protection des données. Selon des statistiques nationales récentes (INEC, 2023), une proportion significative des ménages ruraux et autochtones ne dispose pas d'un accès stable au haut débit. Ce déficit infrastructurel produit une double exclusion : d'une part, l'exclusion des services numériques essentiels ; d'autre part, l'exclusion d'une participation significative aux environnements numériques dans des conditions véritables d'information. Dans les contextes de connectivité limitée, les individus peuvent être contraints d'utiliser des plateformes numériques gérées par l'État – telles que les registres publics ou les systèmes administratifs – sans infrastructure adéquate ni soutien suffisant en matière de littératie numérique, ce qui accroît les asymétries dans le traitement des données et leur supervision.

Plutôt que de présenter cette dynamique en termes rhétoriques comme une « colonisation numérique », cette étude la conceptualise

comme une forme de dépendance informationnelle territorialement différenciée, dans laquelle les régions marginalisées deviennent des fournisseurs de données au sein de systèmes technologiques centralisés, sans bénéficier d'une protection réglementaire ou institutionnelle proportionnelle. Les recherches sur la violence numérique en Équateur et en Amérique latine indiquent en outre que les femmes et les personnes LGBTIQ+ figurent parmi les groupes les plus exposés au cyberharcèlement, au doxxing et à la diffusion non consentie de contenus intimes ou personnels. Malgré cela, les niveaux de signalement demeurent relativement faibles. Les analyses disponibles associent cette sous-déclaration à la méfiance envers les institutions, à la peur de la revictimisation et à l'insuffisance de mécanismes de réponse sensibles au genre au sein des structures chargées de l'application de la loi (Defensoría del Pueblo del Ecuador, 2023 ; OEA y ONU Mujeres, 2022). Cette combinaison d'exposition accrue et de réparation limitée contribue à des formes de revictimisation numérique.

Les données d'enquête suggèrent enfin qu'une part considérable de la population ne possède pas les compétences numériques avancées nécessaires pour exercer effectivement les droits reconnus par l'article 12 de la LOPDP, tels que la rectification, l'effacement ou l'opposition. Si ces droits existent formellement, leur mise en œuvre pratique dépend de la connaissance qu'en ont les citoyens, de leurs compétences techniques et de leur accès aux canaux institutionnels. En conséquence, les individus disposant d'une plus faible littératie numérique peuvent demeurer exposés de manière disproportionnée aux pratiques d'extraction de données sans activer de mécanismes correctifs. En somme, les frontières numériques en Équateur ne sont pas uniquement technologiques, mais structurelles. Alors que les données personnelles peuvent circuler à l'échelle transnationale avec une relative facilité, la capacité d'obtenir protection, réparation ou reddition de comptes institutionnelle demeure contrainte par des inégalités infrastructurelles, éducatives et territoriales. Cette asymétrie renforce

les schémas existants d'exclusion sociale dans la sphère numérique.

4. Souveraineté informationnelle et économie politique de la vulnérabilité numérique en Équateur

Dans le contexte de l'expansion du *big data*, la vie privée en Équateur doit être comprise non seulement comme un droit individuel, mais aussi comme une question de souveraineté informationnelle, c'est-à-dire comme la capacité de déterminer qui collecte, traite, stocke, transfère et, en dernière instance, gouverne les données personnelles dans des conditions de pouvoir inégal. Plutôt que de considérer la vulnérabilité numérique comme un problème purement technique ou administratif, cette section soutient qu'elle résulte d'asymétries structurelles entre infrastructures technologiques, capacité réglementaire, concentration du marché et possibilité inégale, pour les citoyens, d'exercer leur autodétermination informationnelle. En ce sens, le cas équatorien met en lumière un dilemme plus large en Amérique latine :

la connectivité s'étend plus rapidement que les garanties institutionnelles, tandis que la reconnaissance des droits demeure plus faible que les infrastructures d'extraction qui organisent la vie numérique contemporaine.

4.1. Reconnaissance normative et asymétrie infrastructurelle

L'article 66 de la *Constitución del Ecuador de 2008* reconnaît le droit à la vie privée personnelle et familiale, y compris la protection des données personnelles. Cette reconnaissance a été renforcée par la LOPDP de 2021, qui incorpore formellement des principes tels que la limitation de la finalité, la proportionnalité, la légalité et le consentement. Toutefois, cette consolidation normative n'a pas été accompagnée de garanties institutionnelles et infrastructurelles équivalentes.

En 2025, le taux de pénétration d'Internet dépassait 70 % de la population équatorienne, faisant de l'interaction numérique un élément central de la vie économique, politique et sociale. Mais cette extension de la connectivité a aussi accru l'échelle

et la granularité de la collecte de données, notamment en matière de géolocalisation, de consommation, de santé et d'expression politique. Il en résulte un déséquilibre structurel : alors que les droits sont formellement reconnus, les infrastructures qui organisent la vie numérique demeurent largement gouvernées par des systèmes technologiques opaques, des logiques de sécurité publique et des plateformes corporatives transnationales.

Dans cette perspective, le cas équatorien illustre moins une absence de norme qu'une asymétrie notable entre reconnaissance juridique et mise en œuvre opérationnelle. La souveraineté informationnelle apparaît ainsi fragmentée entre promesse constitutionnelle et dépendance infrastructurelle.

4.2. Médiation par les plateformes, surveillance et publicité conditionnelle

Les plateformes numériques ont élargi les possibilités d'expression, de visibilité et de mobilisation, mais elles ont également intensifié la surveillance et la captation des

données comportementales. En Équateur, les réseaux sociaux ont joué un rôle central dans les mobilisations autochtones, les protestations civiques et les campagnes contre les violences de genre entre 2019 et 2022. Cependant, ces mêmes espaces s'inscrivent dans des architectures de surveillance où la communication est continuellement archivée, profilée, modérée et potentiellement réutilisée.

Cette tension ne se limite pas à la censure manifeste. Elle renvoie à une sphère publique conditionnée : un environnement communicationnel dans lequel la parole demeure formellement possible, mais technologiquement médiée par des infrastructures qui façonnent la visibilité, la circulation, la légitimité et le risque. Les systèmes de modération algorithmique opérés par les grandes plateformes, ainsi que les pratiques documentées de logiciels espions dans la région andine, montrent que la communication numérique ne se contente pas de transmettre de l'information mais participe également à la production symbolique de la

réalité et à la régulation du discours public (Silva-Escobar, 2023).

L'enjeu n'est donc pas seulement de savoir si les citoyens peuvent s'exprimer, mais dans quelles conditions technologiques leur expression est stockée, classifiée, monétisée ou surveillée. Le problème relève d'une liberté médiée : l'expression est rendue possible, mais dans le cadre de régimes d'opacité où la conservation des données, le profilage et les usages secondaires demeurent difficiles à auditer ou à contester.

4.3. Inégalité numérique et citoyenneté différenciée

L'inégalité numérique approfondit ces tensions en distribuant la vulnérabilité informationnelle de manière inégale au sein de la population. Les écarts de connectivité, les inégalités de littératie numérique, l'exposition différenciée aux violences en ligne et l'accès limité à des mécanismes effectifs de réparation façonnent des capacités très inégales à protéger les données personnelles et à exercer les droits numériques. En

Équateur, ces asymétries affectent non seulement l'accès aux services numériques, mais aussi la possibilité de résister à l'extraction, de comprendre les régimes de consentement et d'exiger des comptes.

Les femmes, les personnes LGBTIQ+, les communautés autochtones et les populations rurales se trouvent particulièrement exposées à ces environnements, non seulement parce qu'elles y participent dans des conditions inégales, mais aussi parce que les hiérarchies sociales préexistantes y sont reproduites et intensifiées. La vulnérabilité numérique doit ainsi être comprise comme une forme de citoyenneté différenciée : alors que certains acteurs prennent part à la vie numérique avec davantage d'autonomie, de littératie et de protection, d'autres y participent dans des conditions d'exposition accrue et de défense institutionnelle plus faible.

Ces dynamiques résonnent avec des débats plus larges sur le capitalisme de surveillance (Zuboff, 2019), la surveillance liquide

(Lyon, 2018) et la colonialité numérique en Amérique latine. Toutefois, le cas équatorien suggère que la grille d'analyse la plus utile n'est pas seulement métaphorique, mais structurelle. Les données personnelles circulent à l'échelle mondiale avec une relative facilité, tandis que les recours juridiques, la supervision institutionnelle et la reddition de comptes démocratique demeurent territorialement fragmentés et socialement inégaux. La souveraineté informationnelle ne peut donc pas être réduite à la seule localisation des données ni au seul formalisme juridique. Elle doit être comprise comme la capacité des individus et des sociétés à exercer un contrôle significatif sur les infrastructures qui organisent la vie numérique.

En somme, ces éléments montrent que la transformation numérique de l'Équateur est – au-delà d'une histoire d'inclusion technologique – une histoire de gouvernance inégale. La question centrale n'est pas simplement celle de la connectivité, mais celle de la distribution du pouvoir dans des

environnements structurés par la donnée. À cet égard, la vie privée, la liberté d'expression et l'inclusion numérique n'apparaissent pas comme des enjeux séparés : ce sont des dimensions interdépendantes d'un conflit plus large autour de la souveraineté informationnelle en Amérique latine.

5. Conclusions

Cette étude a examiné la trajectoire ambivalente des technologies de la communication en Équateur à partir d'une perspective socio-historique. Si l'expansion du numérique a renforcé la connectivité et l'accès aux services, elle a simultanément intensifié les pratiques d'extraction de données, les pressions institutionnelles et les inégalités structurelles.

La reconnaissance constitutionnelle du droit à la vie privée en 2008, puis l'adoption de la LOPDP en 2021, constituent des jalons normatifs importants. Toutefois, les écarts de mise en œuvre, l'ampleur des clauses d'exception, les capacités institutionnelles

limitées et les flux transfrontaliers de données continuent de restreindre l'effectivité de la protection juridique.

Des cas empiriques tels que Novaestrat (2019), l'usage régional de logiciels espions et les dispositifs de traçage numérique mis en place durant la pandémie montrent à quel point la souveraineté informationnelle demeure fragile. Ces évolutions ne relèvent pas d'un déterminisme technologique, mais d'une asymétrie institutionnelle entre l'adoption rapide des technologies numériques et l'adaptation comparativement plus lente des cadres réglementaires et des mécanismes de contrôle.

Les réformes à venir devraient se concentrer sur le renforcement des capacités institutionnelles, la clarification des clauses d'exception, l'amélioration de la transparence des transferts transfrontaliers de données et l'élargissement des programmes de littératie numérique, en particulier dans les communautés rurales et marginalisées. Des recherches longitudinales supplémentaires

seront également nécessaires afin d'évaluer la manière dont les systèmes d'intelligence artificielle en évolution redéfinissent la gouvernance des données en Équateur et dans la région andine.

Plutôt qu'une « prison numérique » au sens métaphorique, le cas équatorien met en évidence un problème structurel de gouvernance : concilier l'expansion de la connectivité avec une protection effective des droits informationnels dans un contexte d'interdépendance technologique mondiale.

Rôles respectifs des auteurs dans l'élaboration de la contribution :

Auteur/autrice 1 : Conceptualisation ; Investigation ; Rédaction – version initiale ; Rédaction – révision et correction

Auteur/autrice 2 : Méthodologie ; Analyse formelle ; Rédaction – révision et correction

Références citées

CEPAL (2023): *Panorama Digital de América Latina y el Caribe*, Santiago, Comisión Económica para América Latina y el Caribe.

Chile (1999, reformada 2023): *Ley 19.628 sobre Protección de la Vida Privada*, Diario Oficial de la República de Chile.

Citizen Lab (2022): *Reports on Pegasus spyware and digital surveillance*, Toronto, University of Toronto.

Colombia (1991): *Constitución Política de Colombia*, Diario Oficial, Bogotá.

Defensoría del Pueblo del Ecuador (2023): *Violencia de género en el ámbito digital*, Quito, Defensoría del Pueblo del Ecuador.

Deleuze, G. (1990): «Post-scriptum sur les sociétés de contrôle», *L'Autre Journal*, 1.

Ecuador (2008): *Constitución de la República del Ecuador*, Registro Oficial, Quito.

Ecuador (2009): *Ley Orgánica de Seguridad Pública y del Estado*, Registro Oficial, Quito.

Ecuador (2021): *Ley Orgánica de Protección de Datos Personales*, Registro Oficial Suplemento 459, Quito, Asamblea Nacional.

INEC (2023): *Encuesta Nacional de Tecnologías de la Información y Comunicación (ENTIC)*, Quito, Instituto Nacional de Estadística y Censos.

Lyon, D. (2018): *The Culture of Surveillance: Watching as a Way of Life*, Cambridge, Polity Press.

OEA y ONU Mujeres (2022): *Ciberviolencia y ciberacoso contra las mujeres y niñas en el marco de la Convención Belém do Pará*, Washington D.C., Organización de los Estados Americanos y ONU Mujeres. Disponible en: <http://www.oas.org/es/mesecvi/docs/mesecvi-Ciberviolencia-ES.pdf>

Parella, S. y T. Speroni (2018): «Las perspectivas transnacionales para el análisis de la

protección social en contextos migratorios», *Autoctonía. Revista de Ciencias Sociales e Historia*, 2(1), pp. 37–56. DOI: <http://dx.doi.org/10.23854/autoc.v2i1.59>

at the New Frontier of Power, New York, PublicAffairs.

Silva-Escobar, J. P. (2023): «Imagen, poder simbólico y vida cotidiana: Los noticiarios de televisión y la construcción mediática de la realidad social», *Autoctonía. Revista de Ciencias Sociales e Historia*, 7(1), pp. 287–322. DOI: <http://dx.doi.org/10.23854/autoc.v7i1.318>

Superintendencia de Protección de Datos Personales (2024): Informe anual de gestión, Quito, SPDP.

Unión Europea (2016): Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016 (Reglamento General de Protección de Datos – GDPR), Diario Oficial de la Unión Europea.

Zuboff, S. (2019): *The Age of Surveillance Capitalism: The Fight for a Human Future*