Perfiles falsos, bots y verificación en redes sociales

Panorama general

La preocupación por los **perfiles falsos** en redes sociales no es exagerada: las propias plataformas admiten que el problema sigue siendo masivo, persistente y difícil de erradicar. **Meta** estima que en **Facebook** las cuentas falsas representaron menos del 5% de sus usuarios activos diarios en el cuarto trimestre de 2025; además, informó que en 2025 retiró **10,9 millones de cuentas** de **Facebook** e **Instagram** asociadas a centros criminales de estafas y eliminó más de **159 millones de anuncios fraudulentos**, el 92% antes de que alguien los denunciara. **X**, por su parte, reconoce que la manipulación de plataforma y el spam constituyen el principal volumen de sus acciones de enforcement y define como conducta prohibida la creación de cuentas no genuinas, “fake personas” y la coordinación artificial para influir conversaciones. **TikTok** también prohíbe las cuentas engañosas y la interacción falsa, y sostiene que su insignia verificada sólo busca confirmar que una cuenta pertenece a la persona o empresa que dice representar.

El punto central es que el fenómeno dejó de ser apenas una molestia digital. Hoy los perfiles apócrifos funcionan como infraestructura para **estafas**, **suplantación de identidad**, **campañas de hostigamiento**, **grooming**, **desinformación**, **manipulación política** y también para la fabricación artificial de prestigio, alcance o tendencia. Los datos regulatorios y de transparencia muestran que las plataformas combaten este tipo de abusos, pero también exhiben lo contrario: si siguen removiendo millones de cuentas y anuncios engañosos por año, es porque el sistema todavía les ofrece a los actores maliciosos un espacio enorme para operar.

Qué muestra la evidencia sobre manipulación política

La hipótesis de que actores políticos usan **bots**, **granjas de cuentas** o redes coordinadas para influir en la conversación pública no surge de una intuición aislada; tiene respaldo en investigación comparada. El **Oxford Internet Institute** documentó actividad organizada de manipulación en redes en **81 países**, encontró evidencia de uso de **desinformación** en 76, de **bots** en 57 y de partidos o políticos que aplicaron técnicas de propaganda computacional en **61 países**. El mismo estudio advirtió que se gastaron casi **60 millones de dólares** en firmas privadas que emplean bots y otras estrategias de amplificación para instalar mensajes políticos como si fueran tendencias orgánicas.

En **Argentina**, la discusión también dejó rastros verificables. **Freedom House** señaló que la elección presidencial de 2023 tuvo un grado "sin precedentes" de manipulación de contenido online, incluido el uso de **deepfakes**. En su informe sobre **Argentina**, la organización explicó que durante la campaña hubo comportamientos aparentemente organizados mediante **bots**, **trolls** y cuentas personales conectadas a operaciones políticas; además, registró reportes sobre una red de cuentas trolls utilizada para influir la conversación electoral e impulsar publicaciones del entonces candidato **Javier Milei**. El mismo reporte remarca, sin embargo, que el funcionamiento preciso y el financiamiento de esas redes muchas veces permanecen opacos o sin prueba concluyente, y que la desinformación digital durante la campaña también circuló desde otros sectores políticos.

Ese matiz es importante para una columna editorial seria: la evidencia disponible **no permite afirmar que toda la dirigencia política use granjas o bots**, pero sí autoriza una inferencia razonable y periodísticamente defendible: parte del sistema político convive con un ecosistema que le puede resultar funcional, porque las redes coordinadas sirven para amplificar agenda, hostigar

críticos, sembrar ruido y simular climas de opinión. Esa inferencia se apoya en la documentación internacional sobre propaganda computacional y en los reportes argentinos sobre manipulación electoral y redes coordinadas, aunque no debe presentarse como una verdad universal ni como una acusación personal sin prueba específica.

Impacto social, económico y periodístico

El daño más visible aparece en las **estafas**. La **FTC** informó que en 2025 las redes sociales fueron el medio de contacto fraudulento que más pérdidas generó: **2,1 mil millones de dólares**, con un aumento de ocho veces respecto de 2020. La misma agencia señaló que casi el **30%** de quienes reportaron perder dinero en una estafa dijeron que todo había comenzado en redes sociales. Y la propia **FTC** explica que las llamadas **romance scams** suelen arrancar con perfiles falsos en **Instagram**, **Facebook** y otros entornos sociales, donde el estafador construye confianza antes de pedir dinero.

El impacto también alcanza a niñas, niños y adolescentes. El **NCMEC** explica que su **CyberTipline** recibe denuncias por explotación sexual infantil online, incluidas las de **online enticement** y **sextortion**; además, define la captación online como el contacto con alguien que se cree menor con fines de cometer un delito sexual o secuestro, e incluye allí el **grooming** para obtener imágenes sexuales o un encuentro presencial. En **Argentina**, el **artículo 131 del Código Penal**, incorporado por la **Ley 26.904**, pena el grooming, y el portal oficial **Derecho Fácil** recuerda que el delito consiste en contactar a una persona menor por medios electrónicos para cometer delitos contra su integridad sexual.

La **desinformación** es otro frente decisivo. Una encuesta de **UNESCO** e **Ipsos** en 16 países mostró que el **68%** de los usuarios de internet considera que las redes sociales son el lugar donde la desinformación está más extendida, muy por encima de apps de mensajería o medios digitales. En la Argentina, un estudio difundido por el Estado nacional indicó que las noticias falsas se

concentran sobre todo en **política** y **economía**, con el **78,1%** y **43,5%** de las menciones respectivamente. En otras palabras: los perfiles falsos no sólo engañan personas, también contaminan el debate democrático en los temas más sensibles del interés público.

El periodismo tampoco queda al margen. **Freedom House** reportó un aumento del hostigamiento online contra periodistas y usuarios críticos en **Argentina** durante el período que cubrió la elección de 2023 y los primeros meses del nuevo gobierno. Y **FOPEA** informó que en 2023 registró **117 casos** de agresiones a la libertad de expresión, el número más alto en cinco años; luego, en 2025, ese monitoreo marcó un récord de **278 casos** y sostuvo que el poder político seguía siendo el principal agresor de la prensa. No todo esto se explica por perfiles falsos, pero sí ayuda a entender por qué las redes coordinadas y las campañas de hostigamiento se volvieron un problema institucional, no sólo tecnológico.

Regulación, verificación e incentivos cruzados

El marco argentino hoy aparece **fragmentado**. La **Ley 25.326** protege los datos personales y el honor frente al uso indebido de información identitaria, mientras que el Código Penal castiga conductas concretas como el **grooming**. Pero el propio relevamiento legislativo de la **Biblioteca del Congreso de la Nación** muestra que todavía siguen en debate, mediante proyectos separados, la **rectificación de datos falsos en redes sociales**, la **suplantación de identidad digital**, el **hostigamiento digital**, la **autenticación biométrica para menores** y la **responsabilidad de intermediarios en internet**. Eso sugiere que el sistema normativo actual reconoce daños puntuales, pero todavía no consolidó una política integral sobre identidad y trazabilidad en plataformas.

En el plano internacional, la **Unión Europea** avanzó más. El **Digital Services Act** obliga a grandes plataformas a ofrecer mayor transparencia, apelaciones y mitigación de riesgos sistémicos. En ese marco, la **Comisión Europea** abrió actuaciones

contra **TikTok** por riesgos electorales vinculados a la elección rumana y más tarde concluyó que **X** engañaba a los usuarios con su blue check, al permitir que cualquiera pagara por una condición presentada como “verificada” sin comprobar de forma significativa quién estaba detrás de la cuenta. En diciembre de 2025, la Comisión multó a **X** con **120 millones de euros** y sostuvo expresamente que ese diseño dificultaba a los usuarios juzgar la autenticidad de cuentas y contenidos.

Ese caso prueba algo clave para el debate editorial: **no toda verificación es verdadera verificación**. **Meta Verified** afirma que su insignia se basa en actividad en sus plataformas o en documentos/información aportados por el usuario y que ofrece protección contra suplantación. **TikTok** dice que su badge confirma que la cuenta pertenece a la persona o empresa representada. **X**, en cambio, aclara que su check azul significa que la cuenta tiene una suscripción activa a **X Premium** y cumple requisitos de elegibilidad, pero **no** implica que haya sido verificada con documento; la verificación de identidad existe como etiqueta opcional separada. Si el usuario común no puede distinguir esas diferencias, el sello pierde valor cívico y puede transformarse en un emblema de marketing, no de autenticidad.

Ahora bien, la idea de que “si todos los perfiles estuvieran verificados, habría más responsabilidad” tiene una lógica fuerte, pero requiere precisión. Sí: una **verificación robusta** elevaría el costo de la suplantación, dificultaría ciertas estafas y mejoraría la trazabilidad frente a denuncias. Pero la evidencia disponible también indica que la identificación obligatoria no es una bala de plata. La **EDPB** advirtió que los sistemas de verificación o aseguramiento de edad pueden afectar derechos como la protección de datos, la no discriminación y la integridad de las personas. Documentos vinculados al sistema de **Naciones Unidas** subrayan que el discurso anónimo online forma parte de las garantías de privacidad y libertad de expresión. Y la literatura académica sobre políticas de nombre real muestra resultados mixtos: algunos estudios hallaron que estos sistemas no reducen —

e incluso pueden aumentar— ciertas formas de agresión o disminuir la participación y la calidad informativa.

La conclusión más sólida, entonces, no es que haya que elegir entre **anonimato total** o **identificación total**. La evidencia apoya un enfoque más fino: verificación graduada para cuentas de alto alcance o riesgo, trazabilidad y resguardo de identidad ante autoridad competente, transparencia obligatoria sobre automatización y publicidad política, sanciones efectivas para suplantación, y mejores vías de denuncia y reparación. Eso preserva derechos de personas vulnerables que necesitan seudónimo, pero no deja la conversación pública a merced de ejércitos de cuentas descartables.