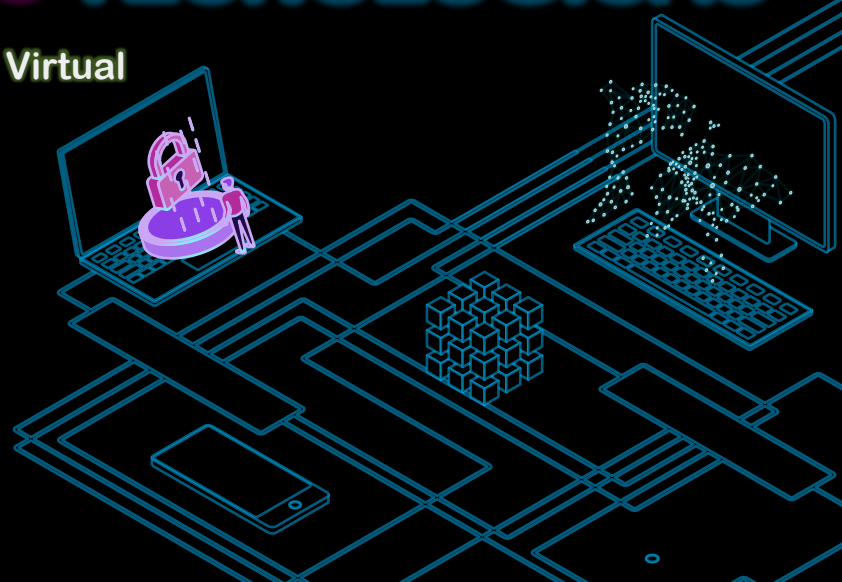
VIOLENCIA DIGITAL Y MAL USO DE DATOS PERSONALES EN PLATAFORMAS TECNOLÓGICAS

Conversatorio Virtual

LUIS GUSTAVO PARRA NORIEGA

Comisionado

@lgparranoriega



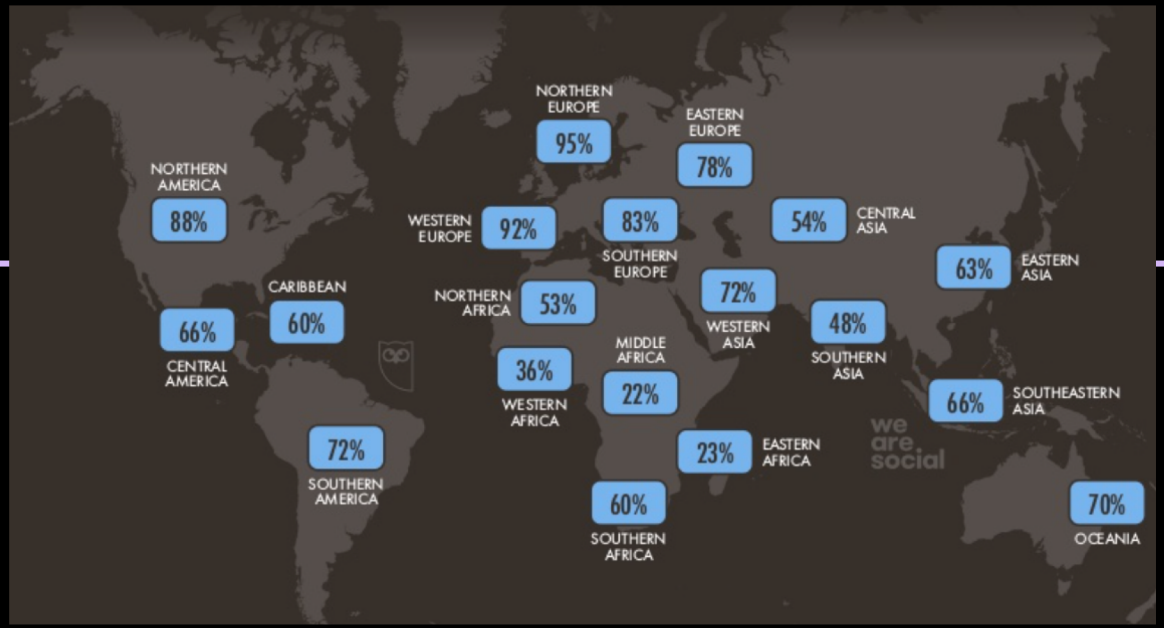
CONTENIDOS

1

USO DE INTERNET

En 2019 el mundo existían **4.388 millones** de internautas, más de la mitad de la población global, en 2020 este número ya alcanza los **4.540 millones, es decir, el 59% de la población mundial**.

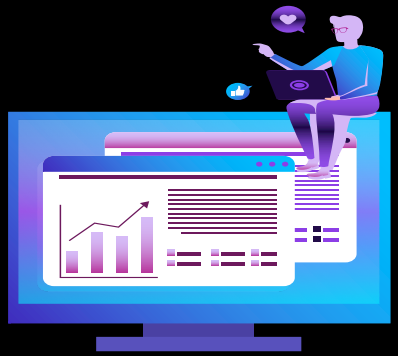
Las dos regiones con mayor penetración de internet en la actualidad son Europa oriental (92%) y el norte de Europa (95%)



Fuente de consulta: Digital 2020 Global Digital Overview (January 2020)

REDES SOCIALES

Los usuarios de las redes sociales han superado la marca de los **3.800 millones** .
Casi el **60 por ciento** de la población mundial ya está en línea, y las últimas tendencias sugieren que *más de la mitad* de la población total del mundo usará las redes sociales a mediados de este año.

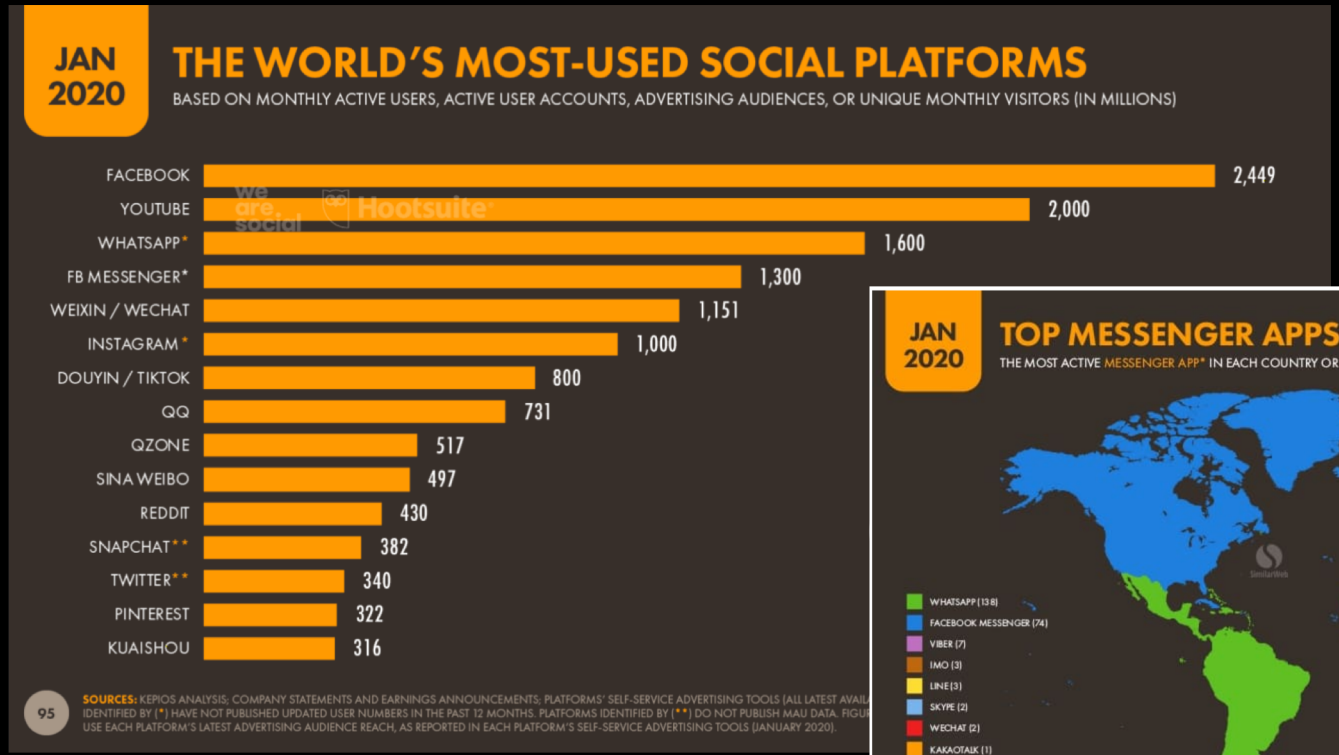


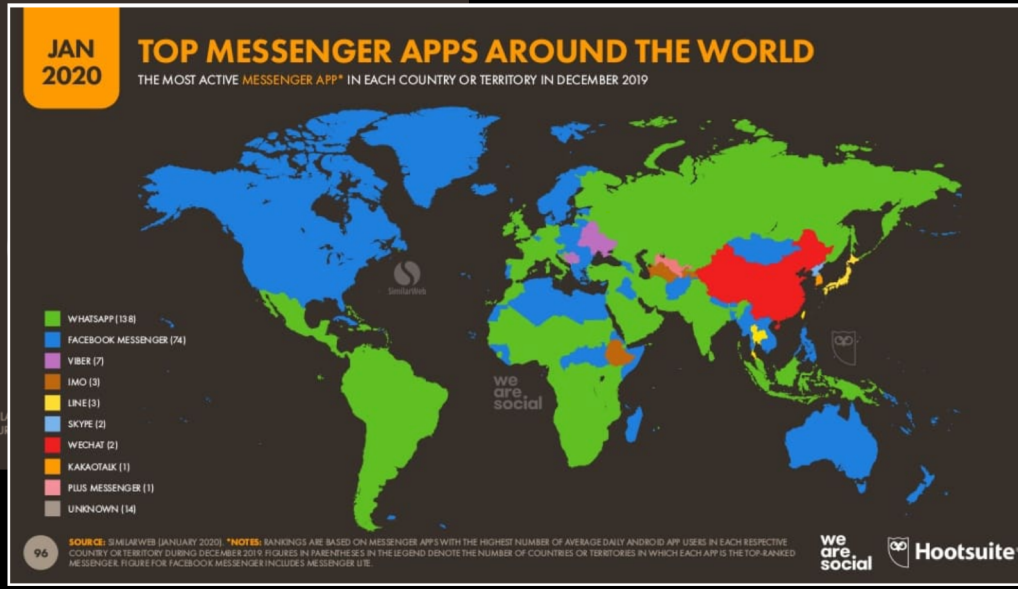
A nivel mundial, más de **5.19 mil millones de personas** ahora usan **teléfonos móviles**

Promedio de conexión al día **6 horas y 43 minutos** (el 40% de nuestra vida despiertos), de las cuales **2 horas y 24 minutos** las usamos solo para redes sociales.

Fuente de consulta: Digital 2020 Global Digital Overview (January 2020)

REDES SOCIALES MÁS USADAS





Fuente de consulta: Digital 2020 Global Digital Overview (January 2020)

En México hay **80.6 millones** de usuarios de internet

86.5 MILLONES DE USUARIOS DE TELÉFONOS MÓVILES

Se estima en **20.1 millones** el número de hogares que disponen de internet (56.4%), ya sea mediante una conexión fija o móvil, lo que significa un incremento de 3.5 puntos porcentuales con respecto a 2018 y de 17.2 puntos porcentuales en comparación con los resultados de 2015 (39.2 por ciento).

51.6% son mujeres.

48.4% son hombres.

Fuente de consulta: ENDUTIH 2019

2

GOBERNANZA DE INTERNET

GOBERNANZA DE INTERNET

La “gobernanza” de internet implica un proceso multipartito en el que todos los puntos de vista se deben tener en cuenta.

Ningún actor puede atribuirse su regulación exclusiva y en los Estados se debe fomentar la cooperación de todos los sectores tanto a nivel nacional como internacional.

Desde 2005 que se realizó en Túnez la Segunda Fase de la Cumbre Mundial sobre la Sociedad de la Información y en la Agenda32 establecieron los siguientes puntos en el Apartado de la Gobernanza de Internet.

En el Punto 46 se exhorta “a todas las partes interesadas a que garanticen el **respeto por la privacidad y la protección de los datos e informaciones personales”**

Fuentes de consulta: Estándares para una Internet Libre, Abierta e Incluyente (CIDH) 2013
México digital.gob

IMPACTO JURÍDICO DE INTERNET

De conformidad con la Ley Federal de Telecomunicaciones y Radiodifusion, en su **Artículo 2, fracción** XXXII**, el Internet es**: Conjunto descentralizado de redes de telecomunicaciones en todo el mundo, interconectadas entre sí, que proporciona diversos servicios de comunicación y que utiliza protocolos y direccionamiento coordinados internacionalmente para el enrutamiento y procesamiento de los paquetes de datos de cada uno de los servicios. Estos protocolos y direccionamiento garantizan que las redes físicas que en conjunto componen Internet funcionen como una red lógica única.

Adicionalmente, se puede considerar que tiene estas ***características:***

- **Jurisdición multiple**
- Se ejerce la Libertad de expresión y el libre comercio
- El respeto a la **privacidad y a la no discriminación** son SOLO principios orientadores del entorno digital.
- En cuanto a lo que se va a entender por lícito o ilícito dependerá de las **legislaciones internas**
- Existe la incapacidad de determinar que clase de usuarios van a acceder a la red, y por tanto determinar si son o no menores de edad, esto casi imposible para los prestadores de servicio como para los propios gobiernos.
- La facilidad con que es posible crear una dirección de correo electrónico o una página web con datos falsos permite **actuar con impunidad** a quienes podían estar sujetos a la Ley.

Fuentes de consulta: Estándares para una Internet Libre, Abierta e Incluyente (CIDH) 2013

LEY FEDERAL DE TELECOMUNICACIONES Y RADIODIFUSION (SCJN)

Regulación
REDES SOCIALES

La regulación de redes sociales digitales es una tarea que corresponde al Estado Mexicano, en conjunto con la comunidad internacional, bajo la coordinación de la ONU, la OSCE, la OEA, la CIDH y la CADHP, por cuanto hace a la tutela de la libertad de expresión y el derecho a la información.

Esto es a semejanza de los trabajos que esas instituciones han llevado a cabo en la regulación de internet, mismos que dieron origen a la **"Declaración de Principios para construir la Sociedad de la Información" y la "Declaración Conjunta Sobre Libertad de Expresión e Internet",** y otros trabajos como el "Informe Anual de la Relatoría Especial para la Libertad de Expresión" de 2013.

OSCE

OEA
Más derechos para más gente

CIDH
Comisión Interamericana de Derechos Humanos

RESPONSABILIDAD DIGITAL

La evolución de los medios de comunicación ha propiciado la difusión de información **más allá de límites fronterizos**, la protección de los derechos consagrados en el artículo 13 del Pacto de San José, en las dimensiones establecidas por la Corte Interamericana de Derechos Humanos, y desde las distintas aristas que derivan del uso de las redes sociales digitales

1. Demanda una **regulación conjunta** a través de normas construidas en la comunidad internacional y direccionadas al interior de los Estados.

2. Es necesario y urgente realizar un **diagnóstico integral** en el que participen autoridades y órganos especializados, académicos, sociedad civil, comunidad técnica, y el sector privado, entre otros actores del ámbito local, dirigido a una escala nacional y posteriormente a un nivel internacional.

3. Desarrollar bases que permitan en principio, la **exigibilidad de los derechos digitales** y, posteriormente en un futuro no muy lejano la justiciabilidad de los mismos.

Fuente de consulta: Voto disiidente INFOCDMX Políticas generales para la difusión de información pública mediante las redes sociales digitales

3

DELITOS INFORMÁTICOS

DEFINICIONES DOCTRINALES

“Aquel que se da con la ayuda de la informática o de técnicas anexas”

Nidia Callegari (1985: p. 115)

DELITOS INFORMÁTICOS

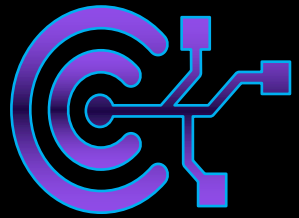
“La realización de una acción que, reuniendo las características que delimitan el concepto de delito, sea llevada a cabo utilizando un elemento informático y/o telemático, o vulnerando los derechos del titular de un elemento informático, ya sea hardware o software.”

Miguel Davara Rodríguez (1996: p. 43)

“...actitudes contrarias a los intereses de las personas en que se tiene a las computadoras como instrumento o fin (concepto atípico) o las conductas típicas, antijurídicas y culpables en que se tienen a las computadoras como instrumento o fin”

Julio Téllez (2004: p. 163)

BIENES JURÍDICOS QUE SE DEBEN PROTEGER EN INTERNET



EL PATRIMONIO, en el caso de la amplia gama de fraudes informáticos y las manipulaciones de datos que da a lugar.

- *LA INTIMIDAD Y CONFIDENCIALIDAD DE LOS DATOS*, en el caso de las agresiones informáticas a la esfera de la intimidad en forma general.

- *LA SEGURIDAD O FIABILIDAD DEL TRÁFICO JURÍDICO Y PROBATORIO*, en el caso de falsificaciones de datos o documentos probatorios vía medios informáticos.

- *EL DERECHO DE PROPIEDAD*, en este caso sobre la información o sobre los elementos físicos, materiales de un sistema informático, que es afectado por los de daños y el llamado terrorismo informático. Por tanto el bien jurídico protegido, acoge a la confidencialidad, integridad, disponibilidad de la información y de los sistemas informáticos donde esta se almacena o transfiere.

Fuente: SANTIAGO ACURIO DEL PINO Profesor de Derecho Informático

CONVENIO DE CIBERDELINCUENCIA DEL CONSEJO DE EUROPA

El Convenio sobre la Ciberdelincuencia del Consejo de Europa menciona en su preámbulo que los **delitos informáticos** son actos dirigidos contra la **confidencialidad**, la **integridad** y la **disponibilidad** de los sistemas informáticos, redes y datos informáticos, así como el abuso de dichos sistemas, redes y datos.

Abierto a firma el 21 de noviembre del 2001 en Budapest

Hasta la fecha, **65** países han ratificado el Convenio.

Objetivos fundamentales:

1. **Armonizar** las leyes penales sustantivas aplicables a las conductas delictivas que tienen como escenario el entorno informático;
2. Proveer reglas de procedimiento penal que brinden a las autoridades nacionales competentes las **facultades necesarias para la investigación y persecución** de tales conductas delictivas; y
3. Establecer un **régimen dinámico y efectivo** de cooperación **internacional**.

Fuentes de consulta: CONSEJO DE EUROPA, Hungría, Budapest, 23/11/2001.
VIOLENCIA DE GÉNERO DIGITAL, por MARÍA FLORENCIA ZERDÁ* y MARINA BENÍTEZ DEMTSCHENKO

TIPOS PENALES VÍNCULADOS CON LAS TECNOLÓGIAS DE LA INFORMACIÓN
Código Penal Federal

ARTíCULO 199 Septies

- **Grooming** (Engaño de adulto a un menor)

ARTÍCULO 200

- **Tráfico de menores** (Comercio de gráficos pornográficos)

ARTÍCULO 202

- **Pornografía infantil** (Obligar a menores a realizar actos sexuales y grabarlos)
- *Relacionado con el artículo 9 del Convenio Budapest Delitos relacionados con la pornografía infantil.

ARTÍCULO 211 Bis

- **Ataques a la integridad de datos** (Alteración o perdidade información contenida en sistemas o equipos)
- *Relacionado con el artículo 4 del Convenio Budapest “Ataques a la integridad de los datos.”

ARTÍCULO 424 Bis

- **Abuso de los dispositivos** (Desactivación de dispositivos electrónicos)
- *Relacionado con el artículo 6 del Convenio Budapest “Abuso de los dispositivos”
- **Cracking informático**
  - (Vulneración de sistemas de seguridad)

PRINCIPALES DELITOS INFORMÁTICOS

Phishing

Infección de sistemas informáticos

Posesión o uso de hardware, software u otras herramientas utilizadas para cometer delitos cibernéticos

Suplantación de identidad

Violencia digital

SUPLANTACIÓN DE IDENTIDAD

EN EL ORDEN FEDERAL:

México está dentro de los 10 primeros países (OCTAVO LUGAR) donde hay mayor incidencia del robo de datos personales, por ello, se buscó sancionar penalmente esta conducta; primero se intentó adicionar en el Código Penal Federal (CPF).

El título vigésimo séptimo, denominado “Delito contra la identidad de personas”, pero solo fue aprobado en la Cámara de Diputados.

El 9 de marzo de 2018, se publicó en el Diario Oficial de la Federación (DOF) las reformas a la Ley de Instituciones de Crédito (LIC), y se contempló el delito de suplantación; también en la reciente Ley de Instituciones de Tecnología Financiera se encuentra previsto, así como en el Código Fiscal de la Federación (CFF), el 1 de junio del año 2019 también se reformó e incluyó el delito de suplantación. A la Ley de Instituciones de Crédito, la suplantación se adicionó en el artículo 112 sextus y séptimus.

Fuente de consulta: SENADO DE LA REPÚBLICA

SUPLANTACIÓN DE IDENTIDAD

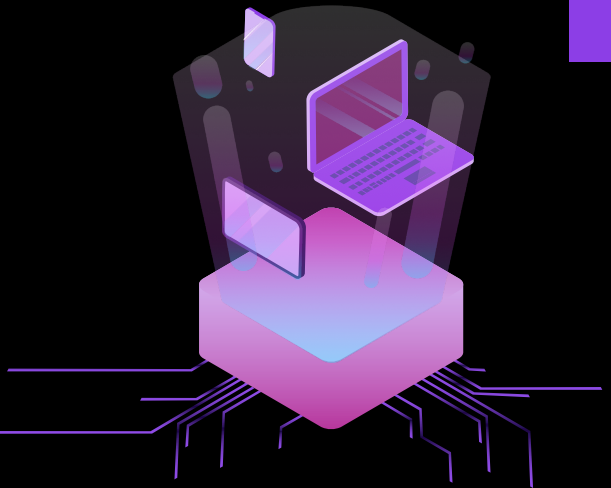
México no cuenta con una legislación federal para sancionar el delito de suplantación de identidad, mientras que a nivel local, solamente **16** Estados de la República Mexicana lo tiene tipificado en diferentes ordenamientos jurídicos.

Estos estados son:

1. Baja California,
2. Baja California Sur,
3. Colima,
4. Chihuahua,
5. Ciudad de México,
6. Durango,
7. Guanajuato,
8. Jalisco,
9. Estado de México,
10. Nuevo León,
11. Oaxaca,
12. Quintana Roo,
13. Sinaloa,
14. Tamaulipas,
15. Tlaxcala y
16. Zacatecas.

Fuente de consulta:SENADO DE LA REPÚBLICA

PERSONA DIGITAL



PERSONA DIGITAL

Persona digital puede definirse como todo aquel individuo que lleva a cabo sus actividades a través del uso de las TICs, dentro de las que se encuentran:

- Correo electrónico
- Banca online
- Comercio electrónico
- Audio y música
- E-administración
- E-gobierno

- Educación
- Videojuegos
- Servicios móviles
- Descarga de música y cine
- Búsqueda de información
- **Socialización (redes sociales)**

Fuente: Consuelo Belloch Ortí. Universidad de Valencia

IDENTIDAD DIGITAL

- Identidad, es “aquello por lo que uno siente que es `él mismo´ [...] es aquello por lo cual sé es identificado”

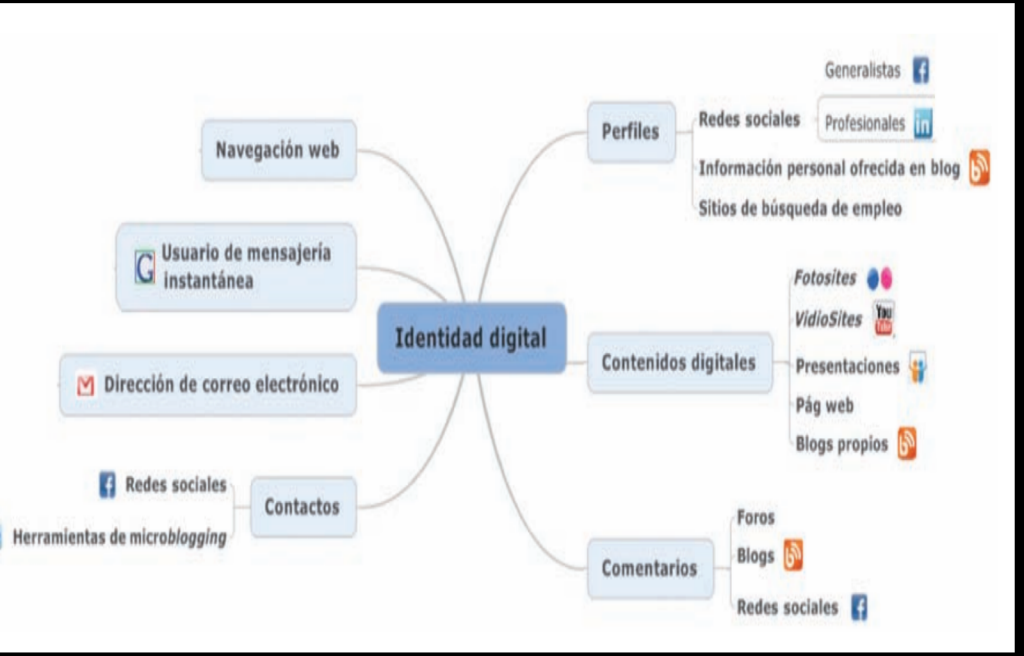
Laing (1961: p.17)

Conceptos importantes para la identidad en la era digital

1. Procesos de socialización (Redes sociales)
2. Privacidad
3. Reputación social
4. **Conductas delictivas por medios electrónicos**
5. E-ciudadano (Persona digital)
6. Preocupación por la protección de datos personales

Fuente de consulta: Identidad Digital: El nuevo usuario en el mundo digital

IMPACTOS EN LA RED QUE CONFORMAN LA IDENTIDAD DIGITAL



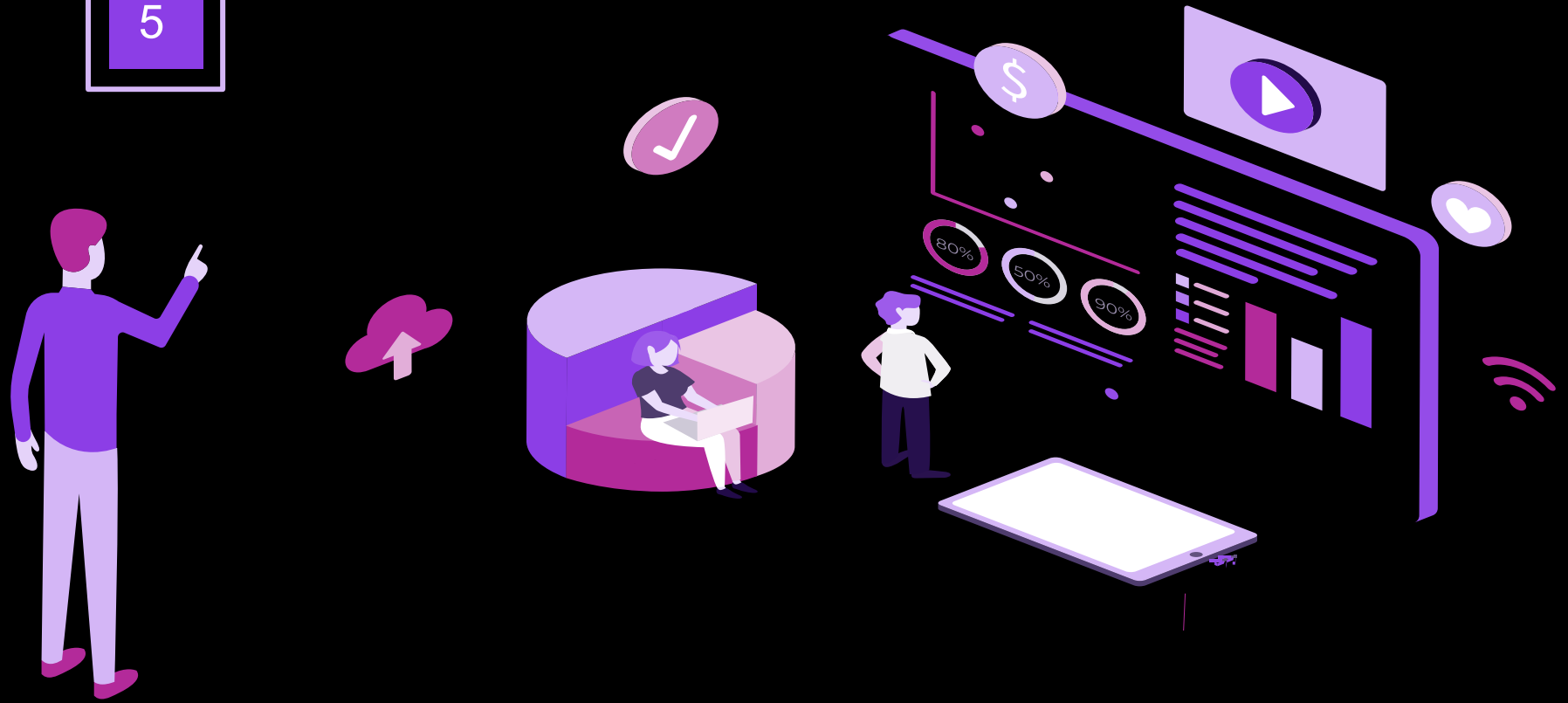
PRINCIPALES PROBLEMAS QUE CONLLEVA

***Robo de identidad**,
*VIOLENCIA DIGITAL
***Afectación en su patrimonio**,
***Discriminación,** de
***Ofertas no deseadas por medios digitales** –*SPAM*- **u otros medios**, por mencionar sólo algunos posibles riesgos.

Fuente de consulta: https://www.gob.mx/cms/uploads/attachment/file/450005/Presentacion_ENDUTIH_2018.pdf

VIOLENCIA DIGITAL

5



PRONUNCIAMIENTO

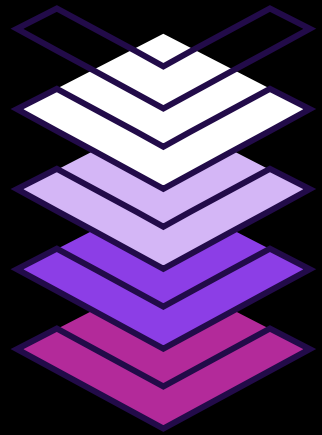
(SNT: 11 de junio 2020)

Bajo un esquema de **coordinación y colaboración con las Instancias del Sistema Nacional**, se emitió **un pronunciamiento hacia las autoridades y ciudadanía para prevenir la violencia digital y mal uso de datos personales en plataformas digitales.**

CONSIDERACIONES PRINCIPALES

En México **hay** 74.3 **millones de usuarios de internet**

- 51.5% son mujeres y 48.5% son hombres,
- Las mujeres jóvenes entre 12 y 29 años son las más atacadas en los espacios digitales



De las agresiones, el 86.3% es cometida por personas desconocidas y el 11.1% por conocidas.

INEGI señala que en 2019 9.4 millones de mujeres de 12 años y más, fueron víctimas de violencia en línea.

PRINCIPALES CONSIDERACIONES

En 2013, la Oficina de las Naciones Unidas contra la Droga y el Delito, efectuó el “Estudio exhaustivo sobre el delito cibernético”, a través del cual desentraña el fenómeno del ciberdelito en una visión integral **cuya responsabilidad en conjunto** abarca a **gobiernos, organizaciones de la sociedad civil, la Academia, el sector privado y la sociedad en general.**

El Convenio sobre Ciberdelincuencia (**Convenio de Budapest**), elaborado en 2001 por el Consejo de Europa, es un tratado internacional vinculante en materia penal que establece herramientas legales para perseguir y sancionar penalmente los ilícitos cometidos, ya sea en contra de sistemas o medios informáticos, o a través del uso de las Tecnologías de la Información y Comunicación (TICs), el **cual es importante que México ratifique.**

Lo anterior destaca serios desafíos a los gobiernos ante la proliferación de conductas ilícitas de carácter cibernético entre ellas la violencia de género ejercida por medios digitales, ha sido un parte aguas importante en México para legislar en la materia con perspectiva de género.

ACCIONES PLANTEADAS

1. Los **Organismos garantes estimamos necesario hacer del conocimiento de las autoridades y ciudadanía que nos mantenemos al tanto de los hechos y actividades inadecuadas realizadas a través de medios tecnológicos, redes sociales y plataformas digitales**, y que se requiere concientizar sobre los riesgos que conlleva un tratamiento ilícito de datos personales y las consecuencias que puede desencadenar para la intimidad y privacidad y dignidad de las personas así mismo, que sean sabedoras de las consecuencias, penales y administrativas, en las que pueden incurrir.

2. Fortalecimiento de **los vínculos con la industria digital,** considerando que la mayor parte de las plataformas digitales y servicios por Internet son prestados por empresas trasnacionales con domicilio en el extranjero, por lo que deberá tomarse en cuenta los **alcances y competencias** en la materia.

3. En colaboración con instancias internacionales colaborar en el diseño e implementación de **mecanismos preventivos y de respuesta**, para reducir el impacto y el daño de cualquier tipo, que se pudiera infligir a las personas afectadas por estos ***fenómenos de violencia digital***, por lo que se necesita apelar a la **responsabilidad ética y social de estas empresas**, para que además de cumplir con la ley se trabaje en la privacidad por diseño y por defecto de todas las aplicaciones o plataformas digitales que desarrollen.

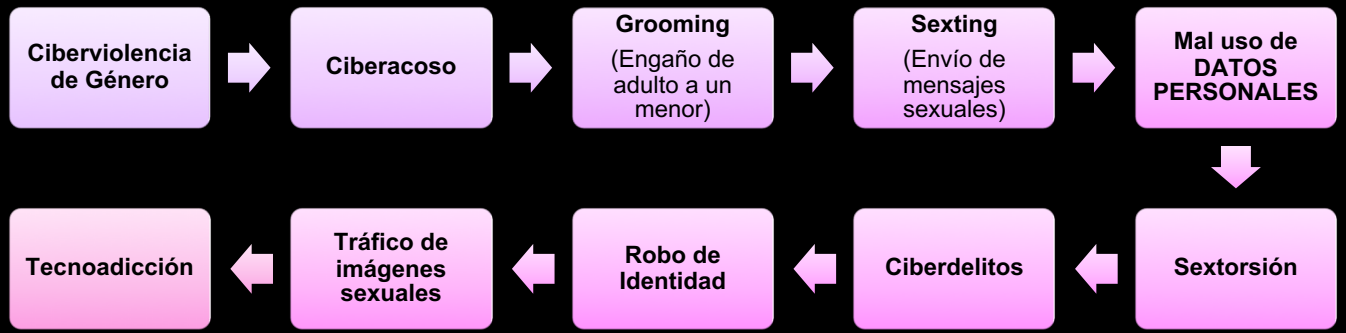
DEFINICIÓN DE VIOLENCIA DIGITAL

De conformidad con la **Ley General de Acceso de las Mujeres a una Vida Libre de Violencia, se define en el artículo 6.** Los tipos de violencia contra las mujeres son:
(De la fracción I a la V)..."**como los actos de acoso**, hostigamiento, amenazas, insultos, vulneración de datos e información privada, divulgación de información apócrifa, mensajes de odio, difusión de contenido sexual sin consentimiento, textos, fotografías, videos y datos personales u otras impresiones gráficas o sonoras, verdaderas o alteradas.

PENAS QUE PROPONE: De **cuatro y seis años de prisión**, multa económica de los **42 mil 245 a los 84 mil 490 pesos**.
*La pena se **agravará** cuando la víctima sea un familiar o tenga una relación de noviazgo, matrimonio o laboral con el victimario.

NO SE ENCUENTRA REGULADO EN EL CÓDIGO PENAL FEDERAL

PROBLEMÁTICAS QUE PUEDEN GENERAR VIOLENCIA DIGITAL



REFORMAS APLICADAS EN ENTIDADES

Conjunto de reformas legislativas encaminadas a reconocer la violencia digital y sancionar los delitos que violen la intimidad sexual de las personas a través de medios digitales, también conocida como **ciberviolencia**. (LEY OLIMPIA)

CONSECUENCIAS DE LA VIOLENCIA DIGITAL

1. Reproche social
2. Afectación de la libertad de tránsito (cambiar recorridos, salir menos o directamente no salir de la casa
3. Modificar aspectos fundamentales de la vida (por ejemplo, cambiar número de teléfono, tener que Avisar a compañeras de trabajo, familiares
4. Daño psicológico inicial
5. Puede implicar otros tipos o modalidades de violencia de género, bullying o ciberbullying.
6. Intentos de suicidio e incluso suicidios consumados.
7. En el caso de la sextorsión, causa detrimento en el plano económico.
8. Las propias víctimas terminan renunciando a sus labores por la vergüenza

6

ACCIONES PREVENTIVAS Y RECOMENDACIONES

ACCIONES PUNTUALES
ESTADO DE MÉXICO

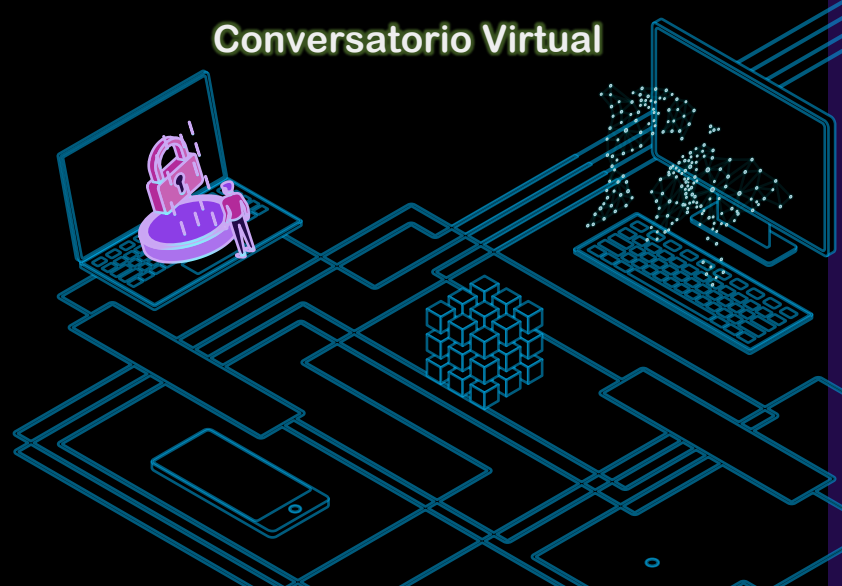
- Trabajo colaborativo con **SIPINNA, Secretaría de Educación, DIFEM y Consejo Estatal** de la Mujer para la capacitación de servidores públicos, profesores de institutos de educación básica, media superior y superior; así como a sociedad civil.
- **Campañas de comunicación** para sensibilizar, concientizar y proteger los datos personales como la integridad digital, así como la transmisión de programas educativos como **Monstruos en Red.**
- En escuelas de nivel básico proponer **esquemas o temática educativa,** con el objetivo de aprender a idéntificar la violencia de género, violencia digital, el uso correcto de las redes sociales.
- Complementar los **protocolos de actuación que tiene la Sria. Educación,** que recoja medidas tanto preventivas como reactivas para combatir la violencia digital.
- Elaborar "**catálogo de riesgos de violencia de género on-line**" y realizar una campaña de divulgación con el apoyo de aliados estratégicos como son la Secretaría de Educación, Órganos Autónomos y Sociedad Civil.
- Elaboración de materiales de divulgación para que la población y sus grupos vulnerables conozcan e identifiquen los **riesgos de violencia digital**, así como sus posibles mecanismos de prevención y defensa ante el abuso en el uso de sus datos personales.

RETOS

- Que las personas reconozcan **conductas de riesgo** a través de medios digitales por el mal uso de datos personales.
- Implementación de un **marco normativo** completo y adecuado para los delitos informáticos.
- Interacción efectiva con los cuerpos de **policía Cibernética y Fiscalías** para la persecución y sanción de delitos relacionados con el mal uso de datos personales.
- Reconocimiento de la violencia digital como una **problemática general** que afecta a toda la población (aunque en mayor medida a mujeres).
- Se requiere la **adhesión al Convenio** de Ciberdelincuencia.
- Legislar fenómenos del **mundo digital**, vínculados con la **violencia** digital.

VIOLENCIA DIGITAL
Y MAL USO DE DATOS PERSONALES
EN PLATAFORMAS TECNOLÓGICAS

Conversatorio Virtual



LUIS GUSTAVO PARRA NORIEGA

Comisionado

@lgparranoriega