



*Asesorías y Tutorías para la Investigación Científica en la Educación Puig-Salabarría S.C.  
José María Pino Suárez 400-2 esq a Lerdo de Tejada, Toluca, Estado de México. 7223898473*

RFC: ATI120618V12

**Revista Dilemas Contemporáneos: Educación, Política y Valores.**

<http://www.dilemascontemporaneoseduccionpoliticayvalores.com/>

**Año: VII      Número: Edición Especial      Artículo no.:138      Período: Diciembre, 2019.**

**TÍTULO:** De la apertura de cuentas de redes sociales y correos electrónicos.

**AUTORES:**

1. Máster. Bolívar David Narváez Montenegro.
2. Máster. Frankz Alberto Carrera Calderón.
3. Ph.D. Jane de Lourdes Toro Toro.

**RESUMEN:** El desarrollo de la tecnología ha ofrecido al mundo nuevas herramientas; sin embargo, estas tecnologías muestran falencias en cuanto a su creación, uso y eliminación inmediata, ya que son reguladas, en su mayoría, por las mismas compañías propietarias de estos servicios web, mediante políticas de seguridad y uso que no garantizan a las personas confiabilidad, proliferando de esta forma, más de 370 millones de cuentas falsas en el mundo, muchas de las cuales sirven a delincuentes para cometer sus actos nocivos y dolosos; esta problemática es el eje de esta investigación que concluye con la propuesta de un marco jurídico regulador para este campo de la informática.

**PALABRAS CLAVES:** red social, usuarios, internet, delito, derechos.

**TITLE:** The opening of accounts of social networks and emails.

**AUTHORS:**

1. Master. Bolívar David Narváez Montenegro.
2. Master. Frankz Alberto Carrera Calderón.
3. Ph.D. Jane de Lourdes Toro Toro.

**ABSTRACT:** The development of technology has offered the world new tools, however, these technologies show shortcomings in their creation, use and immediate elimination, since they are mostly regulated by the same companies that own these services website, through security and use policies that do not guarantee people reliability, thus proliferating, more than 370 million false accounts in the world, many of which serve criminals to commit their harmful and willful acts; this problem is at the heart of this research, which concludes with the proposal for a regulatory legal framework for this field of science.

**KEY WORDS:** Social Network, users, internet, crime, rights.

## **INTRODUCCIÓN.**

La redes sociales, entendiéndose como tal a una comunidad de usuarios que intercambian información de todo tipo, de manera constante e inmediata a través del internet (Fosher, 2014), ha facilitado el intercambio de información de manera casi inmediata y sencilla, pero al mismo tiempo la facilidad para poder crearlas ha sido un hecho aprovechado por muchos cibercriminales para ejecutar actos que lesionan bienes jurídicamente protegidos de otras personas, entre las que se cuentan en gran número menores de edad.

En efecto, el devenir de la tecnología ha cambiado sustancialmente las relaciones interpersonales, haciendo que las personas puedan estar comunicadas de manera casi inmediata independientemente del lugar donde se encuentren con tan solo oprimir un botón o una tecla desde cualquier parte del mundo (Espín, 2015).

También el desarrollo tecnológico ha tenido incidencia en otros campos como en el comercial, haciendo que el comercio sea posible sin necesidad de que el comprador y el vendedor estén en el mismo sitio personalmente y al mismo tiempo. De igual forma, las relaciones políticas entre personas

y entre Estados se ha visto beneficiada con las bondades informáticas que el desarrollo tecnológico ha ofrecido (Quezada, 2015).

En efecto, la información, a diferencia de épocas pasadas, fluye casi de manera inmediata; ya no se debe esperar el transcurso de horas, semanas o meses para tener acceso a cierta información. Aunque medios de comunicación como la televisión y la radio ayudaron y ayudan mucho a la sociedad, transmitiendo información de lo que pasa en cualquier parte del mundo, también es verdad que las personas deben esperar horarios específicos para poder apreciar un noticiero, o deben contar con el artefacto como tal para poder saber sobre una noticia inmediata y urgente, sin perjuicio de que los canales de comunicación se reducen a ciertas estaciones de radio y/ o televisión, frente a decenas o cientos de páginas y/o personas que pueden haber en una red social y en el mismo internet (Francois, 2017)

En efecto, la información cambio rotundamente cuando aparecieron las redes sociales, como un nuevo medio de comunicación por el cual se las personas estarían en contacto constante, sean por mensajes escritos, por fotos y videos que muestren su vida diaria, así como sus acontecimientos de significación personal etc. (Alfonso, 2015).

En efecto, lo que empezó como un proyecto de recreación o entretenimiento entre amigos, empezó a constituirse desde el principio en un medio sumamente poderoso de información, que permite a las personas tener acceso a la información de manera inmediata, solo con contar con un equipo de telefonía celular y datos para su conexión -sin perjuicio de que la señal abierta de wifi en muchas ciudades del mundo ha tomado auge- (Orozco, 2014). Todo esto permitió que lo que empezó como una herramienta de entretenimiento se constituyera en un poder dentro de la comunicación, al grado de que la información de los que pasa en cualquier parte del mundo se comparte y en cuestión de segundos puede ser vista por miles o millones de personas.

Ante esta realidad, las direcciones electrónicas y las cuentas en redes sociales tomaron una forma impensada, hasta constituirse hoy por hoy en el medio de comunicación más influyente en el mundo, al grado de que las acciones de Facebook por ejemplo, han crecido de manera considerable, hasta ubicarle en el top ten de las empresas más e influyentes del mundo, tan solo con unos cuantos años de creación, entre otras causas por la incidencia que tiene en el campo de la publicidad, en vista de los millones de usuarios de tienen creada una cuenta en esta red social (Estrada, 2017).

Ante esta realidad, y debido al poder que tienen las cuentas en redes sociales, la crítica ha determinado algunas falencias que existen alrededor de la apertura, uso y eliminación de estas cuentas. Siendo que, para efecto del presente trabajo de investigación, el análisis se centrará en la apertura de estas cuentas. Ciertamente, cian el aparecimiento de las redes sociales y correo electrónicos que permiten al ser humano tener acceso a la información de manera instantánea y fácil, también han aparecido conductas nocivas por parte de personas inescrupulosas y/o cibercriminales que las utilizan para ejecutar acciones reñidas con la ley, es especial, contra menores de edad quienes pueden ser víctimas de delitos contra su intimidad, su integridad, su vida, etc. (Ramírez, 2018); delitos que resultan más fáciles de cometer para ciertas personas que con un poco de cuidado pueden eludir la responsabilidad penal, civil y/o administrativa que tengan, producto de la utilización dolosa de cuentas en redes sociales (Borich, 2017).

La apertura de cuentas en redes sociales y correos electrónicos es un punto pendiente en la legislación internacional. Éste no es un problema que se arregla tipificando en el cuerpo jurídico de un país las reglas para abrir cuentas en redes sociales, por el contrario, es un problema carácter internacional, dado que las compañías propietarias de las cuentas de redes sociales son extranjeras. Por lo dicho, y por no contar con un consenso mundial por parte de la comunidad internacional, las compañías referidas no han trazados mecanismos que permitan reglamentar la apertura de cuentas, por lo que

una persona bien podría poseer 10, 20, o más cuentas de redes sociales; y no siempre se puede asegurar que su uso va a ser para fines legales.

Ciertamente, algunas cuentas de redes sociales han sido utilizadas para cometer delitos contra la intimidad, el buen nombre, la propiedad, la integridad, y hasta contra la vida de ciertas personas, mismas que han sido objeto de engaños y han visto como una persona escudada en una red social, lesiona bienes jurídicamente protegidos, ya que desde una cuenta de red social falsa, una persona puede cometer estafas, proferir insultos y/ o falsos, engañar a menores de edad sea para seducirles u obtener de ellos prácticas de naturaleza sexual, y hasta organizar citas que pueden terminar con la muerte de la víctima (Hormaza, 2018).

Las ciberconductas criminales descritas son cometidas con más facilidad, ya que los autores no siempre pueden ser identificados, si su conducta la ejecutaron desde una cuenta de red social falsa y desde un computador de un cyber (Piero, 2015).

Las autoridades de justicia se ven impotentes en muchas ocasiones al no poder identificar al titular de la cuenta de red social desde la cual se están generando las acciones dolosas, todos esto porque cualquier persona puede abrirse una. Pero el problema no solo se centra en los criminales que se abren una cuenta de este tipo, sino que también se refiere a las que se abren por parte de menores de edad, quienes quedan vulnerables frente a los cibercriminales. Los casos de menores objeto del denominado grooming, los casos de cuentas falsas que usurpan la identidad de las personas, el número de cuentas desde las cuales se levantas falsos contra otra u otras personas, el número de cuentas desde las cuales se realizan estafas o se apropian de información para fines dolosos, es alta en todos los países del mundo (Bagio, 2018)

Ante la problemática referida, es necesario establecer un marco regulatorio de apertura de cuentas en redes sociales, que permita identificar a los titulares de las mismas, y así poder garantizar derechos como el de la vida, la intimidad, la integridad, la vida, la propiedad, de las personas.

## **DESARROLLO.**

### **Metodología.**

De acuerdo al paradigma descrito en la introducción, la modalidad de la investigación es cualitativa y cuantitativa con tendencia a la primera, ya que se trata de un problema social y se caracteriza por el predominio de la aplicación de métodos teóricos; sin embargo, en la modalidad cuantitativa se aplicó métodos empíricos para la recolección de la información y su interpretación mediante modelos matemáticos estadísticos y en el análisis de las modalidades se emplearon tablas y gráficos.

En cuanto al Tipo de investigación predominantemente se realizó la investigación bibliográfica sobre la base de libros, revistas, monografías e información electrónica actualizados y de autores que se compadecen con el paradigma e investigación. Además, la investigación de campo y documental que permitió aproximarse al problema planteado y sus actores correspondientes.

En cuanto a la metodología se investiga e integra métodos, técnicas e instrumentos en el proceso de investigación en el que predomina el método científico con sus fases esenciales; entre otros:

- La observación directa de los fenómenos, objeto de estudio para identificar el problema.
- Generación de ideas y evaluación de los hechos y fenómenos.
- Evaluación de la posibilidad de que las preguntas científicas e idea a defender se materialicen y se concreten en la práctica.
- Generación de ideas como proceso de innovación teórica y práctica.

Los métodos teóricos más utilizados fueron: inductivo-deductivo, analítico-sintético, histórico-lógico, y enfoque-sistémico.

Los métodos empíricos fueron la observación científica y la medición, el análisis documental y la validación por vía de expertos.

Entre las técnicas más utilizadas fueron entrevistas y la encuesta con los instrumentos correspondientes como son el cuestionario, guía de entrevista, guía y observación.

**Resultados.**

Después de la investigación, que se realizó en producciones doctrinarias hechas por juristas de reconocida sapiencia y en legislaciones que han abordado los problemas que se desprenden del Derecho Informático, se colige que la apertura de cuentas en redes sociales y correos electrónicos debe ser regulado tanto en el Ecuador como en toda la comunidad internacional, ya que no basta con que un solo país convenga con las compañías propietarias de las cuentas de redes sociales, cuando desde otros países, pueden crearse cuentas falsas desde las cuales se puede delinquir.

No olvidemos que muchas estafas, injurias, acosos, pánico, boicot, bullying, suplantación de identidad, etc. que se dan en un país determinado, pueden ser ejecutadas desde otro país, por lo que es necesario que la regulación sea a nivel global, donde todos los países conjuntamente con las compañías propietarias de las cuentas de redes sociales, regulen la creación de éstas cuentas, para garantizar el derecho a la vida, a la integridad, a la honra, a la propiedad, y a la intimidad de las personas (Williams, 2018).

**Resultados.*****Inserción de un marco regulatorio de apertura de cuentas en redes sociales y correos electrónicos.******De la apertura de cuentas en sociales y correos electrónicos.***

Art. 1. Las compañías propietarias de servicio de redes sociales deberán registrar a los usuarios que deseen crear una cuenta, de la siguiente forma:

- La compañía deberá registrar al momento de la creación de cada cuenta la huella dactilar de cada usuario, misma que se guardará en la cuenta del solicitante, y estará a disposición las autoridades de cada país.
- La compañía pondrá la huella dactilar almacenada digitalmente en la cuenta del usuario, inclusive como medio de acceso auxiliar para el ingreso a la misma, sin perjuicio de otros mecanismos

auxiliares de ingreso que cada compañía ponga, de acuerdo a sus códigos y/o políticas de seguridad.

- La compañía deberá registrar los nombres completos de los usuarios, con el detalle de la fecha de la última expedición de su cédula de ciudadanía.
- Las compañías deberán tener interconexión con la base informática de datos de las oficinas de registro de ciudadanía e identificación de los países para corroborar la veracidad de los datos ingresados por el usuario solicitante.

### **Discusión.**

Al incluir en la normativa jurídica de todos los países del mundo una reglamentación para las personas que pretendan crear cuentas en redes sociales y/o correos electrónicos, ayudará a garantizar la seguridad jurídica, ya que ayudará a los órganos de justicia a identificar los titulares de las cuentas desde las cuales se cometen conductas delictuales, los que en la actualidad tienen la facilidad de cometer actos dolosos desde una cuenta donde no constan sus nombres ni ningún indicio verdadero que permita determinar su identidad.

También ayudará a las personas contar con un mecanismo auxiliar de ingreso a las cuentas, en especial aquella que han perdido el control de las mismas al no poder ingresar a ellas, sea porque olvidaron la contraseña y todos los mecanismos auxiliares que permiten ingresar a ellas, o porque un tercero tuvo acceso a la cuenta y la configuró de tal forma que su titular no puede ingresar a la misma utilizando ningún mecanismo auxiliar de ingreso impuesto por la política de seguridad de las compañías. Todo ello, poniendo una opción de reconocimiento de la misma huella dactilar que se empleó para crear la cuenta.



Esto garantizará varios derechos como el de la integridad, la honra y el buen nombre, la propiedad, incluso el derecho a la vida, ya que los cibercriminales no tendrán tan fácil la labor de utilizar cuentas de redes sociales y/o correos electrónicos que contarán con la plena identificación de la persona que maneja la misma, por lo que actos delictivos como la estafa, el acoso sexual de adultos y de menores de edad (particularmente), la usurpación y suplantación de identidad, el bullying, etc. utilizando estos medios, ya no será tan frecuente, ya que las autoridades de justicia corroborarán las huella digital que constará registrada en la cuenta para saber el posible autor del delito.

En efecto, como expresa el Kevin Insúa, la facilidad para cometer delitos empleando redes sociales, se vería colapsada con un mayor control que permita identificar al titular de la misma, mediante la elaboración de códigos, señales o distintivos que le sean propios (Insúa, 2015).

El resultado alcanzado en el presente trabajo de investigación se asemeja al tipo descrito por parte de expertos en seguridad informática, como Kevin Insúa, Valentina Hormaza, Astrid Williams, Andre Miller, quienes han establecido la necesidad de contar con un mecanismo más seguro de creación de cuentas en redes sociales y correos electrónicos, para que se tienda a identificar plenamente a la persona que las utiliza, proponiendo entre algunas recomendaciones, la huella digital como requisito para su apertura, ya que el número de cuentas falsas en redes sociales, se cuentan por millones, Ciertamente, solo la compañía estadounidense Facebook, que ofrece servicio de redes sociales más grande del mundo, ha determinado hasta febrero de este 2019, que más de 370 millones de cuentas son falsas.

La investigación llevada a cabo en el marco de la presente ponencia es novedosa y viable para el Derecho Informático ecuatoriano y, porque establece un marco regulatorio que permita identificar plenamente a la o las personas que utiliza una determinada cuenta de red social o correo electrónico, y que en la actualidad no tiene ningún país del mundo ni lo ha ofrecido ninguna compañía que ofrezca servicios de redes sociales y/o correos electrónicos. Es por esta razón, que la huella digital como

requisito previo a la apertura de una cuenta de red social y/ o correos electrónicos, y como medio auxiliar para ingresar a ellos, así como los nombres del usuario, serán de gran utilidad para la resolución de conflictos mediante la identificación plena del usuario, así también como mecanismo auxiliar para recuperar el control de las mismas.

El resultado presentado en la presente ponencia es práctico desde que tiene la posibilidad de ser legislado en todos los países del mundo, previa modificación de la cuenta, insertando una aplicación o un espacio en la misma cuenta, que permita grabar la huella digital y los verdaderos nombres de los usuarios.

## **CONCLUSIONES.**

La legislación internacional debe contemplar un marco normativo que imponga a las compañías propietarias de las cuentas de redes sociales y correos electrónicos, y así también para sus usuarios, la obligación de registrar la huella digital y nombres verdaderos de sus titulares, esto como requisito que deberá cumplirse en el momento de la creación de cada una cuenta, a fin de garantizar los derechos de las personas, tales como el de honra y el buen nombre, la integridad, el uso exclusivo de la identidad personal, el derecho a la vida, el principio del interés superior de los niños, lo cual incidirá en la disminución de cometimiento de delitos cometidos con empleo de cuentas de redes sociales y/ o correos electrónicos; permitiendo a las autoridades de justicia identificar con más facilidades a los titulares de las mismas, y de esta manera, se evitará la impunidad de muchos de estos delitos que resultan difíciles de sancionar por no poder identificar al titular del espacio web de donde se origina el acto o los actos dolosos, por corresponder a una cuenta falsa, y más si esta es cometida desde un equipo y espacio físico de uso público como ciber o centros de alquiler de computadores.

**REFERENCIAS BIBLIOGRÁFICAS.**

1. Alfonso, D. (2015). Implicaciones jurídicas en el empleo de sistemas informáticos y las nuevas tecnologías”. Editorial del Pencil. México.
2. Bagio, A. (2018). “La usurpación de identidad y el derecho a la protección de imagen”. Editorial Perugia, Perugia.
3. Borich, H. (2017). Los nuevos derechos y el acceso a la tecnología. Editorial Burich. Kiev.
4. Espín, M. (2015). “Las nuevas tecnologías y su incidencia en el mundo contemporáneo”. Editorial Regal. México.
5. Estrada, P. (2017). “El Derecho y su implicación en la Economía y las Finanzas”. Editorial Ramaris. Santiago.
6. Fosher, A. (2014). “The social networks in the world”. Editorial Blu Lagon. Londres
7. Francois, A. (2017). “Los medios de comunicación colectiva”. Editorial Columbo. Buenos Aires.
8. Hormaza, V. (2018). “Las redes sociales y el conglomerado joven”. Editorial francesa.
9. Insúa, K. (2015). “El delito, redes sociales y Derecho informático”. Editorial Arauca. Buenos Aires.
10. Orozco, D. (2014). La Seguridad informática y el cibercrimen. Editorial Arauca. Buenos Aires.
11. Piero, C. (2015). El cibercrimen en el derecho penal contemporáneo. Editorial Perugia. Perugia.
12. Quezada, F. (2015). “La tecnología en el desarrollo del mundo”. Editorial Fernott. Buenos Aires.
13. Ramírez, P. (2018). “El delito y la tecnología del siglo XXI”. Editorial Pascal. México.
14. Williams, A. (2018). “Application of computer security standards”. Editorial The desk and the book. Londres.

**BIBLIOGRAFÍA.**

1. Graciani, M. (2017). Derecho de las nuevas tecnologías. Editorial Arauca. Buenos Aires.

**DATOS DE LOS AUTORES.**

1. **Bolívar David Narváez Montenegro.** Magister en Derecho Civil y Procesal Civil. Docente de la Universidad Regional Autónoma de los Andes, UNIANDES, Matriz Ambato - Ecuador. E-mail: [david\\_narvaez@outlook.es](mailto:david_narvaez@outlook.es)
2. **Frankz Alberto Carrera Calderón.** Magister en Informática Empresarial, Especialista en Auditoría Informática, Abogado de los tribunales de la República, Docente de la Universidad Regional Autónoma de los Andes, UNIANDES - Matriz Ambato - Ecuador. E-mail: [ua.frankzcarrera@gmail.com](mailto:ua.frankzcarrera@gmail.com)
3. **Jane De Lourdes Toro Toro.** Doctora en Ciencias de La Salud en el Trabajo. Docente de la Universidad Regional Autónoma de los Andes, UNIANDES - Matriz Ambato - Ecuador. E-mail: [ua.janetoro@uniandes.edu.ec](mailto:ua.janetoro@uniandes.edu.ec)

**RECIBIDO:** 10 de noviembre del 2019.

**APROBADO:** 19 de noviembre del 2019.