

**UNIVERSIDAD MILITAR
NUEVA GRANADA**



**EDUCACIÓN EN PROTECCIÓN DE DATOS DEL SIGLO XX PARA
SOCIEDADES DEL SIGLO XXI**

**CELMÍ JOHANNA GUERRA BASTIDAS
CARLOS ANDRÉS PANTOJA MEDINA**

Ensayo

WILMAR PEÑA COLLAZOS
Director Extensión y Proyección Social
Representante Investigadores
Facultad de Educación y Humanidades

**UNIVERSIDAD MILITAR NUEVA GRANADA
FACULTAD DE EDUCACION Y HUMANIDADES
ESPECIALIZACION EN DOCENCIA UNIVERSITARIA
BOGOTÁ
2012**

EDUCACIÓN EN PROTECCIÓN DE DATOS DEL SIGLO XX PARA SOCIEDADES DEL SIGLO XXI

CELMÍ JOHANNA GUERRA BASTIDAS¹
CARLOS ANDRÉS PANTOJA MEDINA²

RESUMEN

El ensayo presenta un análisis de la protección de datos en internet y redes sociales de los niños, niñas y adolescentes desde la perspectiva de la educación. Se realiza una presentación de las normas, principios, garantías, sentencias, tratados internacionales y el proyecto de ley sobre protección de habeas data, como mecanismos de protección y respaldo de los menores en protección de datos personales en Colombia. Se realiza un análisis comparativo de las experiencias educativas y las políticas adoptadas en Brasil, la Unión Europea y EE.UU, relacionadas con la temática de privacidad y protección de datos como un análisis de las experiencias realizadas en diferentes regiones. Se realiza una revisión de las acciones y políticas actuales de Colombia y la realidad educativa de los menores en protección de datos en internet y redes sociales. Y por último se plantea una propuesta de acción educativa, a partir de las experiencias exitosas como mecanismo para trabajar en las instituciones educativas a fin de encontrar soluciones reales a la problemática actual.

Palabras claves: *Cibercultura. Educación. Protección de Datos. Menores. Redes Sociales Virtualización.*

DATA PROTECTION EDUCATION OF THE CENTURY XX FOR THE CENTURY XXI COMPANIES

ABSTRACT

The paper presents an analysis of data protection on the Internet and social networks of children and adolescents from the perspective of education. The study presents the rules, principles, warranties, statements, international treaties and the draft law on the protection of habeas data, as mechanisms for protection and support of children in protection of personal data in Colombia. We performed a comparative analysis of educational experiences and policies adopted in Brazil, the European Union and the U.S., the issue related to privacy and data protection as an analysis of the experiences in different regions. A review of the actions and policies of Colombia and the educational reality of minors in internet data protection and social networks. Finally we present a proposal of educational action, from the successful experiences as a mechanism to work in educational institutions in order to find real solutions to the current problems.

Keywords: *Cyberculture. Education. Privacy. Minors. Social Network. Virtualization.*

¹ Abogada de la Universidad Militar Nueva Granada. Especialista en Derecho Comercial de la Universidad de los Andes. Cédula de Ciudadanía 1.085.251.581. Código 1500898. Joha396@gmail.com

² Médico Cirujano. Especialista en Anestesiología y Reanimación de la Universidad El Bosque. Cédula de Ciudadanía 80.870.602. Código 1500904. cpantoja@unbosque.edu.co

El desarrollo de la tecnología y el uso de las nuevas tecnologías de la información y la comunicación son un hecho que enfrentan las sociedades del siglo XXI, lo cual implica oportunidades, conflictos, ventajas y riesgos para la sociedad actual. De esta manera el mundo y las sociedades han evolucionado de manera drástica sobretodo en las dos últimas décadas, vemos ahora que la innovación y la aplicación de la tecnología son utilizadas en todos los campos los cuales quieren mantener un rango de competitividad y Colombia no es ajena a esta implementación de la tecnología, lo cual se ha evidenciado en diferentes estudios realizados desde el año 2000. Es así como de acuerdo con el cuarto boletín trimestral de las TIC 4T 2011, se logra evidenciar que cada año se incrementa significativamente el número de usuarios de las TIC, así: “Al cierre del cuarto trimestre de 2011, Colombia alcanzó un total de 4.836.833 suscriptores a Internet de Banda Ancha Vive Digital y 1.303.438 suscriptores a las demás conexiones a internet, lo cual indica que en referencia al trimestre anterior (3T-2011), el país creció un 3.9% en las suscripciones a Internet fijo y móvil y con respecto cierre de 2010 las suscripciones crecieron un 40.1% al pasar de 4,38 millones a 6,14”. Ministerio de las Tecnologías de la información y la comunicación (2012).

Es por esto que la comprensión de las nuevas culturas implica una integración y comprensión de diferentes factores que influyen en la transformación de la educación y la sociedad, ya que como se plantea actualmente:

“Al final del siglo XX, la evolución societal, marcada por el consumo y la irrupción en la cotidianidad de la tecnologías de la info-comunicación, construye una sociedad hipermediática que incorpora la cultura digital interactiva a sus paradigmas de interacción y transforma las subjetividades juveniles.” (González, 2012).

Lo cual conlleva a que la construcción de las sociedades digitales requieran de un apoyo institucional desde la interactividad que permita conocer y manejar el nuevo lenguaje que en la actualidad presenta grandes falencias debido a que se encuentra basado en subjetividades de los niños y adolescentes que las utilizan.

El mundo del desarrollo y las tecnologías han llevado a la constitución de la denominada cibercultura que en palabras de Levy (2000) es “el conjunto de las técnicas (materiales e intelectuales), de las prácticas, de las actitudes, de los modos de pensamiento y de los valores que se desarrollan conjuntamente en el crecimiento del ciberespacio”(p.1), lo cual implica la implementación y adaptación a este nuevo ciclo de cambio por parte de las sociedades, su comprensión y apropiación mediante diferentes mecanismos educativos que permitan formar a la sociedad en hábitos adecuados del uso de las nuevas tecnologías de la información y la comunicación, o la denominada ciberalfabetización evitando así las denominadas mutaciones tecnológicas.

De acuerdo con el desarrollo de estas innovaciones las organizaciones, empresas y hogares han incluido las tecnologías de la información y la comunicación a sus actividades habituales, generando como consecuencia, que entre ellas las diferentes instituciones educativas hayan establecido políticas que permitan adecuarse al sistema actual,

implementando sistemas como los relacionados con el acceso a canales virtuales, bases de datos, correo electrónico, entre otros, los cuales son aplicables desde el hogar, café internet o trabajo permitiendo interactuar en línea desde los diferentes ámbitos .

Ahora bien, a pesar de que las instituciones han implementado los sistemas mencionados anteriormente, como mecanismo de acción por parte de las entidades educativas, surge un gran interrogante relacionado con la educación en el manejo de las tecnologías de la información y la comunicación, ¿En Colombia existen políticas eficaces relacionadas con la educación actual de las niñas, niños y adolescentes en protección de datos en internet y redes sociales?

Si bien el internet se ha convertido en una herramienta clave de utilización cotidiana por niños y adolescentes, la privacidad, la seguridad, el acceso a contenidos inapropiados siguen siendo puntos críticos que debemos tener en cuenta a la hora de enseñar a utilizar una herramienta tan poderosa (May O. Lwina et al., 2008). Es así como estudios en la actualidad han descubierto la vulnerabilidad a la que inclusive se encuentran expuestos los adultos, al incluir datos personales en la internet y en redes sociales, más aún si hablamos de personas como la población infantil en donde los estudios de privacidad de datos de se ven limitados en algunos países. De esta forma, se hace necesaria una mediación de contenidos en la web que permita generar beneficios claros como por ejemplo ayudar a los niños a entender el medio y los contenidos, aceptar mensajes con su autorización, a intervenir y conocer de primera mano los contenidos y tener clara la relación de esta mediación con el proceso de aprendizaje, toda vez que, en un alto porcentaje de la población infantil no entiende la importancia de la divulgación de datos en la internet y simplemente los suministra.

A pesar de que se ha generado un alto incremento en la implementación de nuevas tecnologías y en el uso de internet se conoce qué es la protección de datos?. Qué es un dato personal?. Pues bien, con el alto incremento del uso de internet y redes sociales se han generado grandes interrogantes; lo cual ha permitido que el estado colombiano haya realizado un desarrollo normativo, el cual encontró diversas falencias, por lo cual se encuentra desde el año 2008 en trámite el proyecto de ley de habeas data. No obstante, el respaldo legal del derecho a la protección de datos personales en la red aún no son conocidas por un alto porcentaje de usuarios. Por lo cual es conveniente iniciar por indicar la definición de dato personal bajo el entendido de la sentencia T- 748 de 2011: “Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables”, lo cual nos indica que toda información que ingrese en la red un niño, niña o adolescente puede considerarse dato personal, información que puede correr muchos riesgos sino es adecuadamente manejada por lo cual se han creado en diferentes estados mecanismos de protección de datos en internet, ya que este tipo de decisiones afectan al niño del presente y al adulto del futuro.

Como consecuencia, el mundo actual ha direccionado su visión hacia la implementación de una reglamentación en materia de protección de datos en la red, lo cual dio sus inicios en el memorándum de Montevideo, donde se presentaron los retos que el período digital enfrenta y los riesgos inminentes que enfrentan los datos de los niños y jóvenes en la red,

requiriendo desarrollar soluciones jurídicas que orienten a las personas y empresas, a fin de que se establezcan compromisos para los estados responsables de sus ciudadanos. De lo anterior, se evidencia la falta de prevención en protección de datos de información personal de niños, niñas y adolescentes en internet y redes sociales por parte de los sitios web, requiriendo una mayor preocupación por parte de los diferentes Estados.

En Colombia, la Constitución Política en su artículo 44 (2010), ha establecido la prevalencia de los derechos de los niños sobre los derechos de los demás, dándole un carácter de fundamental a los derechos de esta población, otorgándole una solides a la protección de los derechos de quienes se consideran más vulnerables en nuestra sociedad. De igual forma, en el artículo 15, de la Constitución se considera el habeas data como un derecho fundamental, el cual se encuentra argumentado y desarrollado en más de 140 sentencias de la Corte Constitucional, donde se establecen diferentes requisitos relacionados con las obligaciones de los administradores de bases de datos relevantes manejados en la red.

De igual forma, en Colombia el Código de la Infancia y la adolescencia regula específicamente los derechos como la vida, calidad de vida, ambiente sano, integridad personal, protección, libertad y seguridad personal, cuidado y custodia personal, identidad, salud, educación, desarrollo integral, intimidad e información (Ley 1098 de 2006) como ejes fundamentales de protección por parte de la familia, la sociedad y el estado. Más aún no se encuentra regulado el derecho a la educación en la protección de datos a los niños, niñas y adolescentes, lo cual ha generado que esta población se encuentre vulnerable a los riesgos actuales que se generan con el uso de internet y redes sociales.

Es así como de conformidad con las reglamentaciones internacionales relacionadas con la protección de datos en la red y las regulaciones colombianas relacionadas con protección de los derechos de los niños, niñas y adolescentes, en Colombia se presentó un proyecto de ley relacionado con el habeas data, el cual surtió su trámite legislativo y constitucional con algunas modificaciones al articulado general. No obstante, se ha mantenido sin objeción alguna el artículo 7 del proyecto de ley estatutaria 184 de 2012 Senado y 046 de 2010 Cámara de Representantes, el cual establece para el estado la obligación de proveer información y capacitar a respecto del tratamiento indebido de los datos personales, el derecho a la privacidad y la protección de la información personal y la de los demás, enfocando la protección de los derechos de los niños, niñas y adolescentes de la siguiente manera:

“Artículo 7°. Derechos de los niños, niñas y adolescentes. En el Tratamiento se asegurará el respeto a los derechos prevalentes de los niños, niñas y adolescentes. Queda proscrito el Tratamiento de datos personales de niños, niñas y adolescentes, salvo aquellos datos que sean de naturaleza pública. Es tarea del Estado y las entidades educativas de todo tipo proveer información y capacitar a los representantes legales y tutores sobre los eventuales riesgos a los que se enfrentan los niños, niñas y adolescentes respecto del Tratamiento indebido de sus datos personales, y proveer de conocimiento acerca del uso responsable y seguro por parte de niños, niñas y adolescentes de sus datos personales, su derecho a la

privacidad y protección de su información personal y la de los demás. El Gobierno Nacional reglamentará la materia, dentro de los seis (6) meses siguientes a la promulgación de esta ley.”

De conformidad con los parámetros legales existentes, la Corte Constitucional mediante su sentencia C – 748 de 2011, realizó un análisis de constitucionalidad al citado proyecto de ley donde en relación con el artículo 7 indicó, que el inciso segundo debía interpretarse que el tratamiento de los datos personales se relacionaban con los menores de 18 años, por ser quienes pueden ser objeto de éste tratamiento, siempre y cuando no se ponga en riesgo la prevalencia de sus derechos fundamentales e inequívocamente responda a la realización del principio de su interés superior. Además, se indica que la opinión del menor siempre se debe tener en cuenta para el tratamiento de sus datos personales. De esta forma, se logran integrar no solo los parámetros constitucionales sino legales para la protección de los derechos de los menores en Colombia.

Ahora bien, bajo los entendidos anteriores se puede establecer que la protección de estos datos especiales, hace que este sea un derecho de especial regulación, por lo cual en Colombia, el estado ha encargado la labor de capacitación en protección de datos a los representantes legales y tutores (entiéndase docentes), por ser el ámbito escolar uno de los más importantes de la vida de los niños, niñas y adolescentes, donde se desarrollan las capacidades de protección de los datos depositados en su actividad cotidiana, ya que actualmente se ha desnaturalizado la noción de internet, lo que ha llevado a preconcebirlo como un espacio sin ley donde las personas pueden actuar sin límites y con la certeza de que siempre se registrará una gran impunidad, lo cual ha sido notoriamente resaltado en el Memorándum de Montevideo.

En este sentido se evidencia, que es el ámbito escolar uno de los más importantes de la vida de los niños, niñas y adolescentes, ya que éste es el principal formador de la capacidad para que los niños puedan distinguir entre los diferentes enlaces en la web, los sitios adecuados y aquellos que no lo son, a fin de que la divulgación de los datos personales en línea tenga una disminución significativa, mediante la mediación activa de los implicados como herramienta eficaz para la protección de la información de los menores en la internet.

En virtud de lo anterior, se observa la necesidad de compromiso por parte los docentes y padres de familia a fin de contribuir a la promoción y divulgación del uso no solo ético sino también responsable de las TIC; Dicha actividad implica la necesidad de familiarización de los docentes (como multiplicadores de la promoción de derechos humanos en internet) con el uso de las TIC y en especial de internet, solo de esta forma podrá lograrse el objetivo del memorándum de Montevideo relacionado con que los niños deber ser: “alertados para no dejarse engañar con la aparente sensación de que en internet todo vale, dado que todas las acciones tienen consecuencias”(Seminarios Derechos, Adolescentes y Redes sociales en Internet, 2009), siendo necesaria la mediación del contenido en la web, que puede generar beneficios claros como por ejemplo ayudar a los niños a entender el medio y los contenidos, aceptar mensajes con su autorización, a intervenir y conocer de primera mano los contenidos. Además permite tener clara la relación de esta mediación con el proceso de

aprendizaje, ya que la mayoría de la población infantil no entiende la importancia de la divulgación de datos en la internet y simplemente los suministra.

A causa de los diversos riesgos que asumen los jóvenes en el ciberespacio como racismo, pornografía infantil, incitación a crímenes contra la vida, homofobia, intolerancia religiosa, striptease, sexting³, grooming⁴, phishing⁵, Cyberstalking⁶, Ciberacoso o cybermatoneo⁷, ciberdelitos⁸, Smishing⁹, Clickjacking¹⁰ entre otros, se han creado diversas organizaciones en diferentes regiones a fin de promover y proteger los derechos humanos en internet, lo cual se ha considerado como una actividad complementaria a las actividades educativas y de orientación que deben adelantar las instituciones educativas para evitar que niños, niñas y adolescentes sean víctimas de los diferentes riesgos que implica el uso de internet y las redes sociales.

³ Sexting: Es cuando alguien toma una foto poco apropiada de sí mismo, provocadora o sexual, y la envía a otra persona vía teléfono celular. El sexting se ha hecho muy popular porque es una nueva forma de exhibirse, coquetear, recibir elogios, mostrar interés o compromiso en una relación. Ministerio de tecnologías de la información y la comunicación. Plan vive digital. EnTicConfio. 2012.

⁴ Grooming: es una nueva forma de acoso y abuso hacia niños y jóvenes que se ha venido popularizando con el auge de las TIC, principalmente los chats y redes sociales. Inicia con una simple conversación virtual, en la que el adulto se hace pasar por otra persona, normalmente, por una de la misma edad de víctima. De esta forma, pretende tener más afinidades con él, gana su confianza y fortalece una supuesta amistad. Esto lo aprovecha el abusador para incluir temas sexuales en las conversaciones, ya sea hablando del tema, intercambiado imágenes eróticas, o haciendo invitaciones para conocerse personalmente. Es en ese momento, cuando se corre el riesgo de un abuso sexual. Ministerio de tecnologías de la información y la comunicación. Plan vive digital. EnTicConfio. 2012.

⁵ Phishing: Es un delito cibernético con el que por medio del envío de correos se engaña a las personas invitándolas a que visiten páginas web falsas de entidades bancarias o comerciales. Allí se solicita que verifique o actualice sus datos con el fin de robarle sus nombres de usuarios, claves personales y demás información confidencial. Ministerio de tecnologías de la información y la comunicación. Plan vive digital. EnTicConfio. 2012.

⁶ Cyberstalking: Este es un tipo de acoso que requiere el uso de las TIC, principalmente Internet. Es parecido al ciberacoso en la medida en que envía continuamente correos y mensajes amenazantes e insultantes a la víctima. Su punto de diferencia está en que aparte de esto, el Cyberstalking investiga y sigue constante la información de una persona o empresa. Es un acto planeado, repetitivo, obsesivo, y no deseado por la víctima. Ministerio de tecnologías de la información y la comunicación. Plan vive digital. EnTicConfio. 2012.

⁷ Ciberacoso o cybermatoneo: El ciberacoso, también conocido como cybermatoneo o cyberbullying, es un tipo de agresión psicológica en la que se usan teléfonos celulares, Internet y juegos en línea para enviar o publicar mensajes, correos, imágenes o videos con el fin de molestar e insultar a otra persona. El ciberacoso no se hace de frente, por eso la víctima no sabe quién puede ser su agresor. Ministerio de tecnologías de la información y la comunicación. Plan vive digital. EnTicConfio. 2012.

⁸ Ciberdelitos: la actividad realizada mediante un computador que es ilícita o que algunas partes considera ilícita y que puede realizarse a través de las redes electrónicas mundiales. Hale, Cybercrime: Facts & Figures Concerning this Global Dilemma, CJI 2002, Vol. 18, available at: <http://www.cjcenter.org/cjcenter/publications/cji/archives/cji.php?id=37>.

⁹ Smishing: Es una variante del Phishing, pero a diferencia de este, usa mensajes de texto para engañar a los usuarios, pidiéndoles información privada e invitándolos a que se dirijan a sitios web falsos que tienen spywares y softwares maliciosos que se descargan automáticamente, sin que el usuario lo note.

¹⁰ Clickjacking: Es una técnica con la que se engaña a las personas para robarles información o tomar control de su computador; esto se hace mediante páginas inofensivas en apariencia, en la que los usuarios deben hacer clic.

De esta forma en Brasil el 20 de diciembre de 2005 se creó SaferNet, como una organización que ofrece el servicio gratuito y anónimo de recepción, procesamiento, direccionamiento y acompañamiento en línea de denuncias anónimas sobre cualquier crimen o violación a los derechos humanos, practicado a través de internet. Lo que ha permitido prevenir y controlar los cibecrimenes a través de capacitaciones que permiten a los niños y niñas conocer los riesgos de publicar datos en las redes sociales o en internet. Esta organización desarrollo las actividades educativas de prevención desde cuatro ejes: investigación y desarrollo, protagonismos, orientación y asistencia y prevención (Gregorio, C. et al 2011).

Bajo este esquema de ejes se logra detectar a partir de los hábitos de navegación en internet de los niños, padres y docentes, las vulnerabilidades y tipos e violación a los DD.HH¹¹ de forma tal que ha permitido la creación de conferencias, talleres, campañas, software, entre otros que permiten capacitar a los niños en los riesgos que corren al ingresar a la red. Así mismo, este mecanismo permite que los estudiantes propongan y evalúen los mecanismos utilizados de tal forma que reflexionen y promuevan las actividades realizadas como mecanismo útil de difusión. Posteriormente, se genera un espacio de orientación y asistencia a aquellos menores que a pesar del asesoramiento y capacitación son víctimas de uno o algunos riesgos de la red, en especial por la falta de consideración de la internet como un espacio público, recibiendo denuncias relacionadas con diversos tipos de agresiones los cuales se manejan por medio de orientaciones y capacitaciones a las víctimas. Finalmente, en el mecanismo de prevención se adelantan capacitaciones a los niños como medio de “intervención social efectiva” (Gregorio, C. et al 2011), el cual permite desarrollar adecuadamente los niveles, cognitivo, social y emocional como se denomina por el autor de los niños que pueden ser objeto de vulnerabilidad.

De esta forma, se realizaron análisis estadísticos en el año 2009 por Safernet (<http://www.safernet.org.br/site/prevencao/pesquisas/jovens>), sobre hábitos de seguridad en la red donde se logro identificar claramente que el 53% de los niños a había tenido contacto con los contenidos agresivos y consideraron inadecuados para su edad, el 38% fueron víctimas de acoso cibernético, el 44% de los amigos 'real' han sufrido acoso cibernético por lo menos 1 vez, el 29% han tenido sus datos robados en línea / perfil y el 26% nunca ningún indicio solicita la protección, lo cual sucede porque el 78% de los de los adolescentes de esta región acostumbra a utilizar internet solos. Todo esto indica la necesidad de la educación de los menores en temas de protección de datos en internet y redes sociales, por lo cual el Gobierno brasileño generó la política de inclusión digital en el cual el mayor enfoque de recursos se encuentran direccionados a educación, el cual inicialmente se enfoca a los docentes como entes que difunden el conocimiento a sus estudiantes con la única falencia de que se capacitan después de que se han hecho efectivo los riesgos en el contexto escolar.

No obstante, al verificar el sistema de capacitación de los docentes se logró evidenciar en el estudio realizado que en una sola jornada era posible capacitar más de 200 educadores por sesión (Gregorio, C. et al 2011), logrando vincular a las autoridades que también deben

¹¹¹¹ Derechos humanos

actualizarse en todos los estados con el fin de conocer y lograr combatir los riesgos, delitos y crímenes e contra de los niños, niñas y adolescentes practicados a través de internet. Estos indicadores nos permiten analizar capacidad que pueden tener los estados de lograr que una política estatal en busca de la protección de datos de los niños, niñas y adolescentes en internet, ya que como lo ha evidenciado la práctica generada en Brasil existe una crisis de valores lo que ha generado el llamado “striptease online de datos” (Remolina. 2010), donde se deja expuesta la intimidad del menor sin tener en cuenta las consecuencias que no solo se pueden generar a futuro sino en su presente, ya que se cada vez se da mas valor a las amistades en la red, aplicaciones de juegos virtuales que desarrollan agresividad y eliminan valores, erotización de los menores, desintegración de las familias por la brecha generacional en tecnologías.

De esta forma en la experiencia de Brasil se identificó que si bien la familia y la escuela eran los únicos referentes en la formación de los niños, hoy los medios masivos de comunicación se han convertido en el eje transversal obligando a las sociedades a adecuar sus sistemas a la realidad social y tecnológica.

Como conclusión de la experiencia de Brasil, se generó la conciencia de que: “los educadores necesitan adecuarse, no apenas a los equipamientos en las escuelas, sino también comprender la dinámica de interacción de las nuevas generaciones de alumnos que establecen con la información y las instituciones sociales” (Gregorio, C. et al 2011). De esta forma, se logra comprender que si bien nos encontramos frente a grandes transformaciones sociales lo más importante es que los docentes se apropien de las tecnologías de la información y la comunicación para orientar a sus estudiantes y prevenir que los niños, niñas y adolescentes sean víctimas de los riesgos de una mala protección de datos en la red.

En Norteamérica la comisión federal de comercio verificó que en la mayoría de los sitios en la web, la protección de datos personales de niños y adolescentes, no merecían privacidad ni importancia por parte de estos; por lo cual se produjo una legislación la cual permitió la reducción de solicitud de información personal innecesaria, como resultado de estos esfuerzos se creó en 1998 la COPPA (Childrens Online Privacy Protection Act), que promovió estamentos diseñados para abolir la recolección de datos personales de niños sin la autorización de los padres o personas a cargo (May O. Lwina et al 2011). Sin embargo pese a que la principal función de COPPA era la del reconocimiento de la vulnerabilidad de los niños en la red y salvaguardar la integridad de los datos de los menores, no ha tenido mayor éxito, ya que después de haberse implementado, solo el 50% de los niños orientados en la web (Turow 2001), cumplían con los parámetros establecidos por ésta. Así mismo, en la actualidad COPPA todavía enfrenta uno de sus principales problemas que es verifica la edad real de sus usuarios.

Ahora bien, el caso de la Unión Europea presenta un avance superior al obtenido en los países Latinoamericanos, no solo a nivel normativo donde se el derecho a la protección de datos de los niños, niñas y adolescentes es un derecho fundamental sino a nivel educativo donde este derecho del alumno es cada vez más protegido por el sistema educativo, el cual desarrolla diferentes estrategias para guiar a los docentes y centros educativos a difundir,

capacitar y desarrollar valores como el respeto en la protección de datos de una población que requiere una mayor protección, generando en el alumno el poder de disposición y control de sus datos personales. De esta forma la comunidad europea a blindado a los centros educativos mediante una armonización de las legislaciones nacionales de los estados miembros, por esto se le dio la categoría de derecho fundamental y democrático, difundidos y aplicándolos en los centros educativos para preparar a la ciudadanía hasta el punto de establecer el día europeo de protección de datos como una nueva cultura social que permita a los niños, niñas y adolescentes tener un poder de disposición y control sobre los datos personales que proporcionan a un tercero.

Finalmente, se han creado agencias para la protección de datos en cada uno de los estados miembros, como medio entre el estado y los centros educativos que permitan desarrollar las destrezas en docentes y alumnos respecto a la protección de datos, ya que día a día se corren riesgos en cuanto a datos de información personal o reservada, ya que como ha sucedido en diversas ocasiones si una empresa comercialmente agresiva invade los datos de un menor, puede muy fácilmente presionarlo durante el resto de su vida con ofertas y promociones adecuadas a su perfil de consumo. De esta forma Jordá indica, que “el sector infantil y juvenil constituye un punto de creciente atención en los últimos años por parte del marketing comercial que lo considera un mercado de gran potencial en expansión” (Consejería de educación de Andalucía, 2011), todo esto indica que si el menor proporciona en el transcurso de su infancia y adolescencia datos que netamente personales a diversos tipos de participantes en la red, esto puede perjudicar su intimidad y la de las personas mas cercanas, y su desconocimiento permite facilitar de forma mas fácil este tipo de datos.

De esta forma, se implementaron diversas políticas en la Unión Europea que permitieron implementar en las aulas la ciberalfabetización, partiendo de la confianza de los docentes en el uso de las tecnologías de la información y la comunicación, ya que los estudiantes asimilaban la seguridad del docente generando calidad y responsabilidad en la información suministrada, ya que tal como lo indicaron estudios del año 2009: “el 44,6 % de los internautas españoles utilizan redes sociales. Por lo que respecta a la segmentación por grupos de edad, la mayoría de los usuarios de redes sociales, siete de cada diez, son menores de 35 años. Un 36,5 % tiene entre 15 y 24 años y un 32,5 % entre 25 y 34. Mayoritariamente son utilizadas para compartir fotografías (70,9 %), enviar mensajes privados (62,1 %) y comentar instantáneas de amigos (55 %), aunque también para cotillear (46,2 %)” (INTECO y la Agencia Española de Protección de Datos, 2009). Lo que ha generó una mayor preocupación por mejorar los mecanismos utilizados para la protección de datos en internet y redes sociales, por lo cual se implementó en las aulas un mecanismo que se desarrolla en cuatro pasos: conocimientos previos, presentación de videos de casos reales, debates guiados y finalmente practicas en internet que permitan al estudiante conocer no solo los riesgos sino también los derechos que tienen en cuanto a protección de datos.

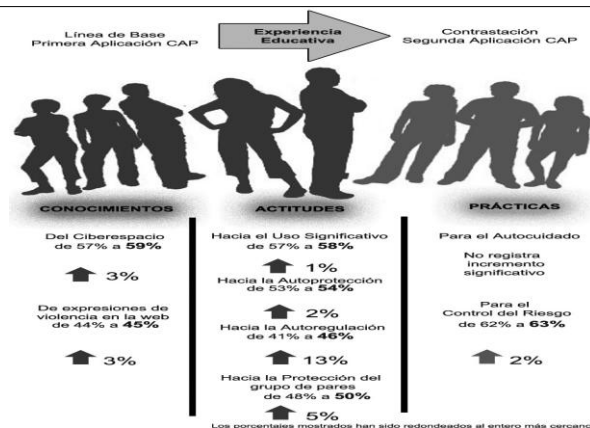
Estos mecanismos han permitido mejorar las condiciones de protección y manejo de datos en internet y redes sociales, lo cual se evidencia en el estudio realizado por el instituto nacional de tecnologías de la comunicación realizado en España en el año 2010, sobre la

seguridad de la información y la e-confianza de los hogares españoles, indicando que: “El 85,3% de los internautas españoles utilizan las redes sociales en el cuarto trimestre de 2010. Estos usuarios prestan cada vez más atención a su privacidad, permitiendo ver su perfil únicamente a amigos y conocidos (67,0%), o a parte de ellos (16,3%)” (INTECO y la Agencia Española de Protección de Datos, 2009), reflejando la adecuada utilidad que han tenido las políticas de educación utilizadas bajo la experiencia europea, mejorando las condiciones de navegación de lo niños, niñas y adolescentes, permitiendo prevenir los riesgos en la red antes de que sucedan mas consecuencias, que en ocasiones pueden resultar funestas para las sociedades futuras.

Finalmente, bajo la experiencia colombiana podríamos decir que si bien en la actualidad se cuenta con políticas que permiten llevar la implementación de tecnologías de la información y la comunicación en regiones apartadas, fue solo hasta finales del mes de agosto del 2012 se creo la nueva política para la protección de datos en internet y redes sociales para niñas, niños y adolescentes por parte del Ministerio de Tecnologías de la Comunicación y la Computación. Lo cual genera como consecuencia que el país no cuenta con una política ya adoptada relacionada con el tema, ni se ha capacitado a los docentes en protección de datos en internet y redes sociales a fin de que éstos, utilicen los mecanismos presentados en la política lanzada como mecanismo de formación de los alumnos, generando la denominada brecha digital generacional, ya que si bien no se han prestado los recursos para capacitar a los docentes tampoco se ha generado una preocupación real por los mismos para manejar el tema, ya que se considera algo ajeno al ámbito educativo.

No obstante, se realizó una experiencia piloto en el Departamento de Cundinamarca bajo la suscripción de un convenio, lo cual permitió conocer en el año 2010 (Secretaría de Educación del Departamento de Cundinamarca/Instituto de Investigación para la Justicia, 2010), que bajo la aplicación de una adecuada política educativa es posible incrementar positivamente el uso adecuado de la protección de datos en internet por parte de los niños, niñas y adolescentes, lo cual se indica en la figura 1 (Gregorio, C. et al 2011):

Figura 1. Proyecto Protección a la Privacidad y Datos Personales de NNA, Cundinamarca, Colombia, noviembre 2010.



Tomado de Gregorio, C. et al 2011. P. 237

Bajo esta experiencia, se partió de la capacitación de los docentes y rectores para pasar a la fase de capacitación de los estudiantes que en caos se amplió también a padres de familia, de forma que permitió llegar a todos los integrantes del medio educativo y lograr una adecuada utilización de las tecnologías de la información y la comunicación.

Con la información suministrada podemos evidenciar la necesidad que en la actualidad tienen las instituciones educativas colombianas de capacitar a sus docentes en tecnologías de la información y la comunicación, de tal forma que logren llegar con seguridad y conocimiento a los estudiantes y estos a su vez logren generar practicas seguras de protección de datos en las redes sociales, conociendo las implicaciones de depositar información personal en las redes sociales.

Como consecuencia de las experiencias analizadas y la situación actual que presenta Colombia en cuanto a educación de niños, niñas y adolescentes en protección de datos en internet y redes sociales, es pertinente considerar la implementación de políticas que lejos de crear paginas web que suministren información a la que voluntariamente será muy bajo el acceso por parte del alumnado, si se requiere que se creen mecanismos desarrollados a partir de cuatro ejes fundamentales:

- a) **Capacitación y Sensibilización docente:** Basada en el desarrollo de competencias del personal docente en manejo de herramientas informáticas y uso adecuado de tecnologías de la información y la comunicación, como mecanismo de desarrollo de habilidades e interés por parte de los docentes, despertando su interés en el uso de internet y redes sociales de forma ética y adecuada.
- b) **Tamizaje estudiantil:** Desarrollado mediante un mecanismo de prácticas donde se hacen pruebas en la red con los estudiantes, para verificar sus conocimientos en protección de datos en internet y redes sociales. De igual forma, se desarrollan mesas de trabajo para discutir y presentar los temas que se desarrollaran y verificar los preconceptos de los estudiantes.
- c) **Presentación de situaciones reales presentadas por rangos de edad:** Mediante el uso de videos, lectura de casos y presentación de casos reales los cuales se categorizan por edades para un adecuado manejo de los riesgos. Así mismo, se realiza un análisis o foro dirigido por el docente basado en las experiencias presentadas y una revisión de la información presentada en la política implementada por el Ministerio de Comunicación y la Información “ENTIC CONFIO”, al igual que visitas en paginas que permitan conocer la regulación actual en protección de datos, permitiendo un adecuado uso a la información presentada por la política gubernamental “ENTIC CONFIO”. Se desarrollan actividades académicas que generen discusión y opinión entre los estudiantes, para aclarar conceptos erróneos y fortalecer aquellos que requieran soporte y acompañamiento.
- d) **Actividades prácticas:** Relacionadas con actuaciones que puedan producir riesgos en la red para los niños, niñas y adolescentes, partiendo de las prácticas realizadas

en las etapas iniciales se desarrollan nuevas actividades prácticas para verificar la adopción de los nuevos conocimientos proporcionados y verificar la actitud de los estudiantes frente al manejo de sus datos personales, generando un comparativo ente los preconceptos y el comportamiento adecuado en las redes sociales e internet.

En este orden de ideas, es necesaria la implementación de políticas públicas nacionales, departamentales y municipales desde el plan nacional de desarrollo para implementar en las instituciones educativas el plan de educación para la protección de datos personales en internet y en las redes sociales de los niños, niñas y adolescentes. Es así como el Ministerio de Educación como ente encargado del manejo de la educación del país debe realizar la implementación y exigencia del programa en las instituciones públicas, de forma tal que estos cuenten con una herramienta de capacitación y protección de los menores bajo su custodia.

Para el caso de las instituciones privadas, si bien cuentan con una autonomía en algunos aspectos, es pertinente aclarar que bajo el parámetro establecido en el proyecto de ley estatutaria de habeas data, se genera la responsabilidad de que *“las entidades educativas de todo tipo deben proveer información y capacitar a los representantes legales y tutores sobre los eventuales riesgos a los que se enfrentan los niños, niñas y adolescentes respecto del Tratamiento indebido de sus datos personales, y proveer de conocimiento acerca del uso responsable y seguro por parte de niños, niñas y adolescentes de sus datos personales, su derecho a la privacidad y protección de su información personal y la de los demás”* (Proyecto de ley estatutaria 184 de 2012 Senado y 046 de 2010 Cámara de Representantes) En consecuencia, se desprende la obligatoriedad de las entidades educativas privadas de capacitar a sus docentes y estos a los niños, niñas y adolescentes sobre los riesgos que corren por un uso inadecuado de sus datos en internet y en las redes sociales, para lo cual es necesaria la exigencia por parte del Ministerio de Educación incluso como mecanismo de acreditación estableciendo este derecho como un eje fundamental en la educación de los menores, para lo cual implementaran los mecanismos mediante la utilización y de recursos propios.

Es posible que no exista una solución absoluta o total, pero es posible mejorar las condiciones de riesgo de los menores poniendo en práctica mecanismos reales de trabajo, ya que es en la práctica en donde se logra obtener los mejores resultados en educación, obteniendo coherencia por parte de los docentes entre lo aprendido y lo enseñado, de forma tal que motiven a los menores y generen en ellos confianza y conciencia del uso ético y adecuado de sus datos personales en internet y en las redes sociales.

Si bien Colombia enfrenta una etapa de “striptease informativo” también se cuenta con las herramientas legales y documentales para poner en práctica una adecuada capacitación en el uso de datos personales en internet y en redes sociales que permita que los niños, niñas y adolescentes prevengan los riesgos antes de ser objeto de los mismos, desarrollando un uso ético de los datos no solo por parte de los menores sino por quienes almacenan los datos, adaptándose mejor a la virtualización de las sociedades. De esta forma, se logrará convertir a los menores de los más débiles a los más fuertes frente a los riesgos y transformaciones,

ya que los dispositivos de comunicación han cambiado y como lo establece Lévy P. (2000) con difusión unilateral, el dialogo-reciprocidad y el multialogo (p.69), los diferentes los tipos de interactividad se han mejorado, generando interconexiones mundiales que se encuentran en un mundo virtual compartido, bajo una inteligencia colectiva la cual ha permitido que las sociedades evolucionen a la medida de las implementaciones tecnológicas.

Para concluir, podemos decir que a partir del recorrido conceptual y comparativo se ha logrado identificar claramente que existe la necesidad de replantear los modelos, prácticas y recursos de categorización, intervención y asesoramiento educativo como solución efectiva y estable a las crisis y conflictos que en la actualidad atraviesa la cibercultura y en la cual se encuentran inmersos los niños, niñas y adolescentes, como víctimas de la brecha digital generacional y de la falta de políticas gubernamentales educativas que permitan una implementación adecuada de la protección de datos en las redes sociales e internet. De igual forma se logra establecer que los docentes cuentan con un reto muy alto relacionado con la mutación contemporánea del saber como lo afirma Pierre L. (2000), donde los docentes tienen el reto de renovar sus saberes y habilidades de tal forma que encarnen el conocimiento que van enseñar a los menores y estos a su vez desarrollen habilidades en el manejo de sus datos y de sus derechos, como mecanismo de evolución a la cibercultura.

REFERENCIAS

- I seminario euro iberoamericano de protección de datos. (2009) La protección de los menores. Cartagena.
- Código de la Infancia y la adolescencia
- Constitución Política de Colombia
- Corte Constitucional de Colombia. SENTENCIA C-748 DE 2011 O HABEAS DATA INTEGRAL
- Consejería de educación de Andalucía. (2011). Guía de protección de datos de carácter personal para los centros de enseñanza. Cona Grafica, SL.
- González, G. (2012) Revista del Instituto para la Investigación Educativa y el Desarrollo Pedagógico, IDEP. 18. P. 21
- Gregorio, C. – Ornelas, L. (compiladores) (2011). Protección de datos personales en las redes sociales digitales: En particular de niños y adolescentes. México. 1.
- Hernández, M. Revista de la agencia de protección de datos de la comunidad de Madrid. http://www.madrid.org/cs/Satellite?c=CM_Revista_FP&cid=1142584110511&esArticulo=true&idRevistaElegida=1142582100339&language=es&pag=3&pagename=RevistaDatosPersonales%2FPage%2Fhome_RDP&siteName=RevistaDatosPersonales
- Instituto Nacional de Tecnologías de la Comunicación (INTECO) y la Agencia Española de Protección de Datos. (2010). Estudio sobre la seguridad de la información y la confianza de los hogares españoles.
- Ley 1098 de 2006. Capítulo II, artículos 17 al 34.
- Lévy, P. (2000) CIBERCULTURA. Informe al Consejo de Europa
- May O. Lwina,1, Andrea J.S. Stanaland and col. Protecting children’s privacy online: How parental mediation strategies affect website safeguard effectiveness. Journal of retailing 84 (2, 2008) 205–217
- Memorandum de Montevideo
- Ministerio de las Tecnologías de la información y la comunicación. Boletín Trimestral de las TIC Banda Ancha Vive Digital (2012). Cifras cuarto trimestre del 2011. Bogotá.
- Proyecto de ley estatutaria 184 de 2012 Senado y 046 de 2010 Cámara de Representante

Remolina, N. (2010, 15 al 20 de noviembre). “Striptease” Informativo, redes sociales, ley de protección de datos personales y ética empresarial. *Ámbito Jurídico*, p.p 12

Turow, Josep (2001). “Privacy Policies on Children’s Websites: Do They Paly by the Rules?”. Philadelphia, PA: The Annenberg Public Policiy Center, available at <http://www.asc.upenn.edu/usr/jturow/PrivacyReport.pdf>

Safernet. Estudio sobre hábitos de los jóvenes. <http://www.safernet.org.br/site/prevencao/pesquisas/jovens>

Secretaría de Educación del Departamento de Cundinamarca/Instituto de Investigación para la Justicia (2010), Protección de la privacidad y datos personales de los niños y adolescentes usuarios de la web: Informe de Resultados, Colombia.

Seminarios Derechos, Adolecentes y Redes sociales en Internet. Montevideo 27 y 28 de julio de 2009