

‘Impacto de los Datos Personales en la Sociedad’



Departamento de Derecho de las Comunicaciones y Tecnologías de la Información.

Universidad Externado de Colombia

14 de marzo de 2025

Bogotá D.C., Colombia

Compilado por

Jaider Jael Morales Torres

Universidad Externado de Colombia

© Universidad Externado de Colombia

Calle 12 No. 1-17 Este

Bogotá D.C., Colombia

Teléfono: 282 60 66 Ext.1105, 1106

esdercom@uexternado.edu.co

“El contenido de esta obra corresponde al derecho de expresión del (los) autor(es) y no compromete el pensamiento institucional de la Universidad Externado de Colombia, ni genera su responsabilidad frente a terceros. El (los) autor(es) asume(n) la responsabilidad por los derechos de autor y conexos contenidos en la obra, así como por la eventual información sensible publicada en ella” Bogotá, Colombia.
Marzo 2025.

Introducción

Cada vez son más frecuentes las noticias sobre los peligros a los que estamos expuestos en materia de privacidad respecto del manejo inadecuado de los datos personales. También, de los riesgos que se derivan por la aplicación de nuevas tecnologías, y como en múltiples de ellas, por el beneficio que representan se omite que son alimentadas para su entrenamiento de grandes bases de datos. Es por ello que el foro tuvo por objetivo resaltar las herramientas que la Constitución y la Ley colombiana contemplan mecanismos de protección a los titulares de los datos personales y a su vez y conocer las aplicaciones que actualmente hacen uso de esta tecnología para el procesamiento de datos.

Se pudo conocer en voz de los expertos en la materia: los avances en la protección de los derechos derivados del tratamiento de los datos personales. De la mano del ejercicio de la acción de tutela ante la Honorable Corte Constitucional, como ente garante de la protección de los datos los titulares de los datos y la aplicación de los principios éticos como límite de los avances obtenidos por la aplicación de las nuevas tecnologías en sectores como las telecomunicaciones y la atención en el servicios de salud.

Agenda del día:

Instalación
Sandra Ortiz Laverde. Directora del Departamento de Derecho, Comunicaciones y Tecnologías de la Información de la Universidad Externado de Colombia.
Dionisio De La Cruz. Docente investigador del Departamento de Derecho Comercial de la Universidad Externado de Colombia.
Disertación respecto de la protección del Derecho de Habeas por parte de

la Corte Constitucional. La Historia Clínica, la defensa del derecho a la intimidad personal y familiar en las actuaciones judiciales y el antecedente penal.
Alexei Julio. Docente investigador del Departamento de Derecho Constitucional de la Universidad Externado de Colombia.
Estado actual de la protección de datos personales. Desde la perspectiva institucional y doctrinaria de la Autoridad.
Carolina García Molina, Directora de Investigaciones de Protección de Datos Personales Superintendencia de Industria y Comercio.
Panel: Aplicaciones del dato que generan bienestar.
Moderador: Dionisio Manuel de la Cruz Camargo
Panelistas: Martha Oyuela. Médica Radióloga - Avances en la medicina a partir del tratamiento de datos, José Leonardo González - Una visión ética del manejo de los datos personales y su aplicación frente a los consumidores, Guillermo Cruz - Datos de salud de <i>Wearables</i> en Colombia, Germán Combariza - Aplicaciones de Ciencia de Datos e Inteligencia artificial en salud

Apertura e Instalación del evento

El evento fue instalado por la Dra. Sandra Milena Ortiz Laverde, – Directora del Departamento de Derecho, Comunicaciones y Tecnologías de la Información de la Universidad Externado de Colombia quien explicó la estructura del evento e indicó que el evento buscaba que las discusiones en materia de datos sean lideradas también por la Universidad Externado de Colombia y que esto se convierta en una fuente de conocimiento para contribuir a la construcción de las diferentes iniciativas legislativas que se van a dar en materia de protección de datos y que hace necesaria la participación activa de la academia.

Seguidamente, el Dr. Dionisio de la Cruz dio sus palabras de instalación, donde mencionó que, desde la Oficina de Protección de Datos de la Universidad Externado de Colombia, se quiso dar la oportunidad a la comunidad estudiantil y todos los demás interesados en el tema, para ofrecer un escenario de discusión sobre la importancia de sus datos, para conocer todas las ventajas y avances que estas tecnologías conllevan. Anticipó que el evento iba a permitir mirar cómo la Ley, Constitución y entidades están encargadas de proteger los datos de los connacionales para garantizar que se utilicen sin vulnerar nuestra intimidad. Para paralelamente, ver los avances que se tiene a la mano a partir del manejo adecuado de los datos personales en diferentes sectores.

Disertación respecto de la protección del derecho de Habeas por parte de la Corte Constitucional. La Historia Clínica, la defensa del derecho a la intimidad personal y familiar en las actuaciones judiciales y el antecedente penal.

El Dr. Alexei Julio Estrada, realizó un recuento de la evolución jurisprudencial tanto de la Corte Constitucional como de la Corte Interamericana de Derechos Humanos (CIDH) en relación con el derecho al Habeas Data. Hizo la aclaración de que el tema es muy extenso, por lo cual, sólo haría referencia a algunos de los temas que ha abordado la jurisprudencia de la Corte Constitucional y una mención específica a la sentencia del caso del colectivo de abogados José Alvear Restrepo contra Colombia. En la cual la Corte IDH determinó que la ley de inteligencia y contrainteligencia vigente en Colombia no se ajustaba a los estándares internacionales en la materia y pidió que fuese modificada como medida de reparación. Respecto de la sentencia referenciada, resaltó que tocó un punto muy importante respecto al manejo y control de datos personales.

A continuación, explicó que las discusiones respecto al habeas data, parten del artículo 15 de la Constitución. El cual establece el derecho a la intimidad, buen

nombre y lo relativo al habeas data o autodeterminación informática. Mencionó que se ha criticado la denominación de “habeas data”, porque el “habeas” tradicionalmente se ha asociado con garantías constitucionales y aquí estaría asociado a un derecho autónomo. Si bien se trata de un derecho autónomo, puede entrar en relación con otros derechos, a veces presentándose colisiones y también casos en que este derecho se ejercita a través de otros derechos, como el derecho de petición. Adicionalmente, explicó que la garantía de este derecho termina siendo la acción de tutela y por eso hay tanta jurisprudencia sobre el particular.

Paralelamente, puso de presente que inicialmente los conflictos se originaron por datos de carácter financiero, crediticio y comercial. Que comenzaron prácticamente desde la misma instalación de la Corte Constitucional por el año 1992, época en la que iniciaron las discusiones respecto a las anotaciones que tenían las centrales de datos sobre la calificación de deudores y estado de créditos. Ese tipo de litigios llevó a la expedición de la Ley 1266 de 2008 para regular esa modalidad de datos. Posteriormente se expedieron las Leyes 1581 de 2012 y 1621 de 2013 que guardan relación con el tema de datos que se almacenan, entre otras normas.

De manera seguida, el panelista, sostuvo que la sentencia que inició la línea jurisprudencial sobre datos que no son de carácter financiero, crediticio y comercial fue la sentencia T-729 de 2002. Esta sentencia sentó las categorías conceptuales que han servido de derrotero al legislador y la propia Corte. El caso fue de un ciudadano que demandó al catastro de Bogotá y a la Superintendencia de Salud, porque decía que en esas bases de datos con sólo ingresar su número de cedula, se obtienen otra serie de datos que violan su intimidad y ponen en riesgo su seguridad. Por ejemplo, en el Catastro, se podía obtener la información de todos los inmuebles que tenía con ubicación y el pormenor de detalles, en general era demasiada información.

Insistió en que la sentencia de referencia es relevante porque si bien trae algunos de los precedentes relacionados a los datos y su protección, avanza en otros temas,

sobre todo en sistematizar de una forma mucho más clara los principios que rigen el tema de datos. En segundo lugar, la Corte desarrolla la tipología sobre la información que contienen los datos que es la misma tipología que ha manejado la Corte en los pronunciamientos posteriores hasta la actualidad. El Dr. Alexei especificó que esa tipología se clasificó en: Información pública, semi privada, privada y reservada, esto se utilizó como criterio para determinar cuándo debe prevalecer el derecho al habeas data frente a otros derechos y viceversa. Mencionó también que frente a cada clase se hizo una categorización. El disertador mencionó que la categorización generó algunos problemas porque fue una sentencia muy incipiente y algunas cosas no quedaron en las categorías que debían quedar.

Respecto a la solución del caso concreto, el Dr. Alexei indicó que la Corte, por una parte, analizó la actuación del catastro y encontró que el problema se relacionaba con que la base de datos de esta entidad violaba el principio de finalidad y necesidad, los datos que aparecían no estaban relacionados con la finalidad de la base de datos y no eran necesarios para los propósitos y fines de la base. En relación con la base de datos de la Superintendencia de Salud encontró que se trata de datos semiprivados que se relacionaban con elementos como el estado civil, relaciones de parentesco y demás, y que entonces no podía haber un acceso público ilimitado a los datos por el carácter que tenían, entonces la regla de resolución de los casos es distinta por el tipo de datos relacionados. Sobre este tema, el Dr. Alexei concluyó que la sentencia tuvo un impacto muy grande, porque las leyes posteriores utilizaron las mismas clasificaciones de la sentencia.

A continuación, hizo referencia a otras líneas jurisprudenciales. En primera medida, la referente a las bases de datos públicas pero que eran consultadas por privados y determinaban sus conductas, sobre todo en materia de acceso al empleo, específicamente bases de datos de antecedentes penales. El problema es que era una base de datos de acceso público que permitía ver si una persona tenía procesos o decisiones en materia penal, lo que generó muchos conflictos y dio lugar a

muchísimas tutelas llevando a que la Corte Constitucional mediante sentencia SU-458 de 2012 unificara los criterios jurisprudenciales.

En los casos objeto de pronunciamiento de la sentencia referenciada, los actores ya habían cumplido las penas o se había extinguido la acción penal, sin embargo, aparecía en la base de datos la leyenda: "REGISTRA ANTECEDENTES, PERO NO ES REQUERIDO POR AUTORIDAD JUDICIAL". Esta base de datos era consultada por muchos empleadores lo que hacía que sus posibilidades de ser contratados fueran mínimas. La discusión se centró en si los antecedentes era un dato personal, que clase de dato eran y si podía haber un acceso público a ese dato. La Corte dijo que sí es un dato personal, que la base de datos era una base de datos personales y que todo el mundo podía acceder a esa información. La Corte resolvió analizando la función que tiene el dato y de las posibles finalidades legítimas o ilegítimas que podría tener el dato.

La Corte indicó que recopilar antecedentes puede tener una finalidad legítima desde la perspectiva constitucional, sin embargo, el problema era el acceso público que se daba a esta base de datos y que se utilizaba como criterio para contratar o no a alguien. Lo que ordenó la Corte es que se cambie la manera en que se arrojan los datos cuando son consultados por el público, que se muestre sólo que la persona no es requerida por autoridad judicial, no que se excluya toda la información porque esa no era la solución, ya que la base de datos cumplía otras finalidades legítimas, por ejemplo, con fines migratorios.

Seguidamente, el conferencista trajo a colación la sentencia T-509 de 2020 que se relaciona con la base de datos de la Fiscalía, respecto de la cual, explicó que es una base de datos de personas que tienen investigaciones penales en curso, quienes en principio, cuando consultan la base de datos de la policía, no sale esa información, pero la base de datos de la fiscalía no es de acceso público, ya que no es lo mismo que haya una investigación penal a que se tengan antecedentes penales, lo que permite cumplir con finalidades diferentes. Pese a que la base de

datos no es pública, se determinó que hubo filtraciones, donde empresas de seguridad en el marco de contratación de particulares tuvieron acceso a esa base y con eso dieron información a futuros empleadores. El problema es un uso ilegal de la información de una base de datos que no es de acceso público. La Corte concluye que los particulares no pueden tener acceso a esa base de datos y si lo hacen están infringiendo la constitución y las leyes.

Posteriormente, el disertador habló de la sentencia T-024 de 2014. Sostuvo que el problema de esta sentencia era el de una ciudadana que había sido condenada, había ido hasta casación penal y había perdido, entonces cuando se googleaba su nombre, aparecía en la página web de la rama judicial, particularmente de la Corte Suprema de Justicia y si se entraba ahí, se podía ver la sentencia con el nombre de ella, esto es problemático porque en la primera decisión la Corte dijo que las providencias judiciales son públicas, y este era el argumento fuerte que se esgrimió acá como defensa. No obstante, lo anterior, con fundamento en una vulneración al derecho al trabajo al no ser contratada por la información que aparecía, la Corte decidió que debe reemplazarse el nombre de la señora en la sentencia, por una sucesión de letras o números que impidieran su identificación.

A continuación, se expusieron dos sentencias que se refirieron a la solicitud de información por periodistas a universidades públicas sobre funcionarios públicos, las sentencias T-324 de 2024 y T-454 de 2024, en la cual piden dos tipos de información, información sobre el título e información sobre el estatus académico de la persona. En ninguna de las dos sentencias se piden calificaciones, sin embargo se puede entender del *obiter dicta* de la segunda sentencia que incluso se puede pedir calificaciones.

El Dr. Alexei comentó que, en los dos casos, la Corte resolvió utilizando más o menos los mismos criterios. La Corte señaló que en las solicitudes se pide dos tipos de datos que están en las bases de la universidad. Un tipo de datos que es de carácter público que es el dato del título, pero que el dato del estatus académico es

semiprivado y en ese sentido, no es de libre acceso, sin embargo, la Corte dice que hay que tener en cuenta el contexto en el que se pide, por una parte, se trata de un funcionario público, respecto del cual, hay jurisprudencia que explica que su derecho a la intimidad no tiene el mismo alcance del de una persona que no ostenta la calidad de funcionario público. En segundo lugar, esas personas ejercen un cargo de responsabilidad pública y, por tanto, el público tiene un interés legítimo en saber sobre su idoneidad y los méritos académicos que tienen para ejercer en ese cargo. Y, en tercer lugar, que la información en ambos casos es pedida por periodistas y la Corte privilegia el derecho de los periodistas a acceder a la información.

Con base en todo lo expuesto, la Corte hizo un juicio de ponderación y llegó a la conclusión de que, en estos casos, el derecho a la intimidad y habeas data debe ceder ante la libertad de acceso a la información y, en consecuencia, la universidad estaba obligada a entregar la información del título y el estatus académico.

Por último, el Dr. Alexei ilustró acerca de la sentencia de la Corte IDH en el caso del Colectivo de Abogados José Alvear Restrepo (CAJAR) contra Colombia. Los hechos consistieron en que CAJAR fue objeto de seguimiento durante mucho tiempo por organismos de inteligencia y seguridad de Estado colombiano. El problema específico fue que algunas de esas actividades de seguimiento se dieron bajo la vigencia de la ley 1621 de 2013 de inteligencia y contrainteligencia, se discutía si el marco legal que permitía desarrollar esas actividades se adecuaba a los estándares internacionales en la materia y la Corte determinó que no, porque la ley es muy amplia y no define varios puntos importantes donde lo que más llamaba la atención es que la mayoría de esas medidas aunque implicaban el acceso a datos de carácter reservado, no requerían autorización judicial previa, sólo excepcionalmente en algunos casos era posterior. Adicionalmente existía la figura del monitoreo del espectro electromagnético que implica necesariamente interferir en la libertad de comunicación privada, lo que generaba otro problema.

El expositor manifestó que la Corte IDH argumentó que toda esa ley es contraria a los estándares y dentro de las ordenes que dio al Estado colombiano en el marco de las garantías de no repetición fue modificar esa ley. Finalmente, comentó que el Estado colombiano en este momento está en supervisión de cumplimiento de esta sentencia y se espera que cumpla la orden de adecuar el ordenamiento e incorporar lo dicho en la sentencia respecto de los estándares internacionales en la materia.

Conferencia ‘Estado actual de la protección de datos personales. Desde la perspectiva institucional y doctrinaria de la Autoridad.’

A continuación, la Dra. Carolina García Molina, Directora de Investigaciones de Protección de Datos Personales de la Superintendencia de Industria y Comercio realizó una presentación que tuvo como objetivo explicar cómo hace la autoridad de protección de datos (Superintendencia de Industria y Comercio) para garantizar la protección de derechos fundamentales como el habeas data.

De manera inicial, la expositora explicó que las funciones de la Dirección de datos personales, tiene un componente de vigilancia y control frente a los obligados de las leyes sobre habeas data que son la 1266 de 2008 y 1581 de 2012. A continuación, detalló las funciones mencionadas, explicó que las funciones abarcan la supervisión y control de organizaciones tanto públicas como privadas, asegurando que estas respeten los derechos de los ciudadanos en materia de protección de datos. Además, la autoridad brinda orientación clara y accesible a individuos y entidades, explicando sus derechos y obligaciones. También, en casos de incumplimiento, lleva a cabo investigaciones rigurosas y aplica sanciones cuando corresponde, lo que no solo disuade prácticas ilícitas, sino que también repara los derechos de los afectados. Estas acciones pueden iniciar por el titular de los datos o de oficio por parte de la Dirección.

La Directora explicó que en el marco de supervisión y vigilancia, se hace un seguimiento del registro nacional de bases de datos, el cual permite identificar ciertos comportamientos a través de la información mínima que se requiere para hacer la inscripción, y tomar decisiones frente a lo que los responsables en ese registro incorporan de información para que la dirección tome medidas administrativas. Mencionó que normalmente el responsable de realizar el registro suele verlo como una carga, pero si bien es un método para que la Superintendencia haga seguimiento, también permite que el responsable haga un análisis interno de su organización y le permite adoptar medidas para mejorar la protección de datos personales, mejorar sus bases de datos y sus medidas de seguridad. Esto permite que no sea solo una obligación sino una manera de auto seguimiento y autorregulación frente al cumplimiento de la norma.

La expositora comentó la percepción de la Dirección de investigaciones frente al tratamiento de datos que se está llevando a cabo por los responsables haciendo uso de las nuevas tecnologías. Indicó que hay muchos negocios a través de IA, herramientas tecnológicas que permiten mejorar las organizaciones, sin embargo, se percibe desde la Dirección que se está tratando en el tema de datos sensibles la excepción como la generalidad.

Sostuvo que, en casi todas las aplicaciones y herramientas tecnológicas, se están tomando datos sensibles, por alguna razón, sin embargo, ante el volumen de aplicaciones que hacen esto, la excepción de la ley 1581 de datos sensibles, se está volviendo el uso general y cualquier cosa implica tratamiento de datos sensibles. Desde la Dirección se está tratando de evitar esta problemática, están prontas a salir algunas ordenes frente a este tipo de comportamientos en algunos responsables, donde no sólo se deben dar sanciones pecuniarias, sino ordenes que permitan que efectivamente haya modificaciones a los procedimientos en cuanto a la exigibilidad de que el dato sensible sea sólo de manera excepcional como lo menciona la ley y que se cumplan los requisitos legales para poder tratar estos datos personales.

Adicionalmente, explicó que, dentro de la implementación de las nuevas tecnologías, se ha evidenciado que el tema de la autorización es muy importante para que se tenga en cuenta, puesto que generalmente se presentan las denominadas autorizaciones sombrilla, donde se da autorización para todo y nada, la finalidad específica y clara es poco frecuente.

Seguidamente, la expositora, trajo a colación los retos que tiene la Autoridad de protección de datos personales. El primero es la adaptación a nuevas tecnologías, ya que el rápido avance tecnológico exige una constante actualización de conocimientos y herramientas para abordar las nuevas formas de tratamiento de datos y los riesgos asociados a la privacidad. Otro reto importante es la concientización y formación, pues resulta esencial educar a ciudadanos y organizaciones sobre la relevancia de la protección de datos personales, proporcionándoles los recursos necesarios para ejercer sus derechos y cumplir con sus obligaciones. Finalmente, se mencionó la cooperación internacional, dado que la protección de datos es un tema global que requiere la colaboración entre autoridades de distintos países para asegurar la privacidad y seguridad de la información en un mundo cada vez más interconectado.

Para concluir la intervención, explicó que las normas relativas a la protección de datos no están obsoletas para nada, tienen unos principios muy generales que permiten manejar el tratamiento de datos en Colombia de mejor manera, aunque sí es necesario actualizar el régimen que se tiene en este momento. Así pues, el objetivo como entidad es propender por la expedición de una modificación a la ley 1581 de 2012 donde se incorporen aspectos importantes sobre nuevas tecnologías, la posibilidad de ser autoridad de protección de datos personales no solo para empresas colombianas sino también para las extranjeras, frente a las cuales la Superintendencia ha estado bastante limitada sobre todo para llegar al tema sancionatorio. Adicionalmente, el reto que se tiene es llegar a disponer todo el apoyo logístico, personal y de experiencia de la Superintendencia para que cada vez más

responsables tengan la posibilidad de hacer sus negocios de manera tranquila, donde no tenga que estar la autoridad encima y estar supeditados a esa vigilancia y supervisión, sino hacer que los obligados puedan tener una autorregulación, no es fácil porque no todos tienen esa misma intención, pero comentó que se está trabajando en integrar a todos los actores en espacios que permitan avanzar en esos cambios.

PANEL: Aplicaciones del dato que generan bienestar.	
Moderador	Dionisio Manuel de la Cruz Camargo
Panelistas	Martha Oyuela. Médica Radióloga - Avances en la medicina a partir del tratamiento de datos. José Leonardo González - Una visión ética del manejo de los datos personales y su aplicación frente a los consumidores. Guillermo Cruz - Datos de salud de Wearables en Colombia. Germán Combariza - Aplicaciones de Ciencia de Datos e Inteligencia artificial en salud. Alejandro Rodríguez – Líder de la Unidad de negocio de imágenes diagnósticas de Philips, North Hispanic.

Palabras iniciales

El Dr. Dionisio de la Cruz introdujo el tema y dijo que el panel estaría estructurado por una pequeña presentación de cada panelista sobre lo que hacen y el sentido teórico práctico de lo que es la recolección y tratamiento de datos, para luego, hacer

una ronda de preguntas enfocadas en los temas que tienen que ver con la protección y tratamiento de datos y las tecnologías expuestas. Indicó que para el desarrollo del panel, primero se abordarían los límites éticos en general en el manejo de datos y herramientas de IA, luego la parte aplicada sobre el tema de qué es un algoritmo y cómo se llega a una instancia de IA, ya que muchos no tienen idea de cómo se alimenta el algoritmo de los datos personales y por qué razón hay que protegerlos, y una vez se tuviera claridad de los temas anteriores, se pasaría a ver en qué consiste la herramienta de medicina de precisión y finalmente cómo todo se utiliza en la práctica y cuál es el impacto que se tiene de esto.

El primer panelista en intervenir fue José Leonardo González, quien habló sobre los temas éticos y filosóficos de la aplicación de las herramientas de IA. Explicó desde su visión de filósofo que a partir del avance de las nuevas tecnologías, se ha mostrado muchos nuevos campos de aplicación para principios que se tenían en otros contextos pero que se pueden expandir a estos nuevos fenómenos. Indicó que durante su intervención explicaría cuáles son los principios básicos en los que se está moviendo el tema de la ética desde la filosofía y las ciencias sociales en general.

En primera medida, dijo que el análisis debe partir de reconocer que hay repercusiones positivas y negativas del uso de la IA y la cuestión ética surge como una posibilidad de lo que debería ser esa repercusión. La gran pregunta es: cuáles son esos valores que se deben defender en el uso de la IA. Hizo mención de los instrumentos que dan luz sobre esos principios, como la recomendación de la OCDE de 2019, la recomendación sobre ética de la UNESCO de 2021 y la ley de IA de la Comisión Europea de 2021. Mencionó que en Colombia salió el CONPES de IA como un avance importante ya que cuenta con un fundamento ético interesante.

Con base en los instrumentos mencionados, pasó a explicar cuáles serían los fundamentos éticos más importantes. Primero, explicó que los instrumentos se fundan en el respeto por los derechos humanos, equidad, seguridad, transparencia,

responsabilidad, trazabilidad e inclusión, principios reinterpretados para la IA. Por otra parte, la importancia de la colaboración internacional. Respecto a la ley de IA de la Comisión Europea, expresó que presenta una categorización del tipo de acciones, que se basa en un principio de daño y establece que los usos de la IA se pueden categorizar en esa pirámide de daños. Sostuvo que los usos de la IA deben estar reglamentados a partir de la posibilidad de ese daño, es decir, cuando hay riesgo mínimo, la intervención debe ser mínima, mientras que, en casos de riesgos inaceptables, no se permitan estos usos.

Continuando con su presentación, el panelista explicó que cuando se habla de ética de la IA, se confunden dos preguntas que hay que distinguir, la primera es ¿Cómo usamos los seres humanos la IA de manera ética? y la otra es ¿Cuál es la ética de los sistemas de IA? es decir, cuáles son los valores con los que vamos a diseñar, una está enfocada en los usuarios y la otra en los diseñadores.

Adicionalmente, mencionó que hay unos supuestos éticos que son el punto de partida. El primero es que los seres humanos somos libres y el segundo supuesto es la instrumentalidad de la IA, es decir, que la IA no es un agente ético, no se le puede atribuir autonomía y responsabilidad, es sólo un instrumento, para cerrar, dijo que se puede sintetizar todas las recomendaciones, leyes y directrices de la IA, en cuatro grandes principios:

1. Principio de daño, que consiste en que no se debe dañar a otro.
2. Principio de Beneficencia: no sólo no se debe dañar, sino que se debe beneficiar, al ser humano, comunidad o medio ambiente, entre otros campos.
3. Principio de autonomía: cualquier uso de la IA si o si debe estar supervisado por una persona competente, en este sentido, los sistemas de IA no son agentes, no son autónomos. Adicionalmente, se protege a las personas de la manipulación o determinismo digital.
4. Principio de justicia: que la IA beneficie a la mayor cantidad de personas.

A continuación, se dio paso a Germán Combariza quién explicó en su intervención cómo funciona la IA y por qué los datos son importantes. Para iniciar, hizo una mención al concepto de datos, explicó que no son algo sólo numérico, sino que va hasta las emociones que demuestro y otros tipos de información. Un dato es una palabra muy amplia, donde entran conceptos de distintas áreas como el derecho y la ingeniería entre otras. Luego, respecto del funcionamiento del algoritmo, señaló que entre mejores sean los datos, mejor será el algoritmo y que van a existir los sesgos porque como humanidad tenemos sesgos y los estamos pasando a la máquina.

Seguidamente, el panelista mencionó los proyectos en los que se está trabajando desde la Universidad Externado en temas de algoritmos, donde, por ejemplo, se ha estudiado el caso de la creación de contenido falsa a partir de algoritmos y su identificación a través de algoritmos también, donde se llegó a la conclusión de que es muy difícil, pues a medida que el algoritmo que identifica avanza, el algoritmo que crea el contenido avanza también y evade la detección del otro.

En este punto, el moderador tomó la palabra para indicar que la IA se puede usar en una variedad de actividades, respecto de las cuales surgen muchas preocupaciones, por ejemplo, los temas de consumo, específicamente de la manera de cómo se comportan los individuos con determinados estímulos. Indicó que durante la discusión se tocarían algunos de esos temas específicos de usos de la IA, por ejemplo, la siguiente presentación que fue de la Dra. Martha Oyuela quién hablaría de la medicina de precisión.

La panelista inició su intervención con la explicación de que la medicina de precisión se está desarrollando y el objetivo es que en Colombia se promueva un proyecto que permita su uso y adopción. Sostuvo que la medicina de precisión va a redefinir nuestro destino porque al tener mayor precisión y poder anticiparnos al desarrollo de enfermedades, vamos a cambiar el enfoque médico, pasando de una medicina reactiva a una preventiva. Explicó que la medicina de precisión toma en cuenta la

variabilidad individual de los genes, el entorno y estilo de vida de cada persona, lo que permite predecir con mayor precisión estrategias de tratamiento y prevención para una enfermedad en particular, resaltó que en estos procesos, el dato es fundamental.

Para profundizar sobre el funcionamiento de la medicina de precisión, explicó que se hace una secuenciación genómica, donde es importante tener claro que cada individuo es único y esa diferencia es la que trata de ver la medicina de precisión, ya que habrá personas que por sus características genéticas no responden a los mismos tratamientos que otras con patologías similares, por tanto, habrá que hacer modificaciones que dependen de la variación genética. Entonces, la medicina genómica es la parte central de la medicina de precisión, porque se toman los genes y se ve según sus características que posibles enfermedades se llegarán a desarrollar, para con esto, trabajar en prevenir específicamente esas enfermedades de manera anticipada.

A continuación, ilustró acerca de la farmacogenómica, donde la industria busca saber que medicamento dar a un grupo de personas y que realmente les sirva, por ejemplo, en cáncer de pulmón hay un medicamento que lo puede detener si se identifica de manera temprana. Resaltó que recibimos de nuestra familia muchas características, pero no quiere decir que ya estemos condenados a padecer esas enfermedades ya que existe la epigenética, la cual permite identificar y trabajar en unos mecanismos diferentes a la secuenciación genética que hacen que se produzcan unos cambios que hacen que respondan los genes de manera diferente, por ejemplo, cosas en el medio ambiente que hacen que se disparen esas predisposiciones o también determinados hábitos que las inhibe.

Para continuar, la panelista recalcó que no hay medicina de precisión sin IA y ciencia de datos porque en estos procesos se genera una cantidad de datos gigante que necesita de ciencia de datos. Finalmente, explicó que en el funcionamiento de la medicina de precisión, todos los datos que se recogen de los cambios y secuencias

en el organismo permiten encontrar maneras de mejorar los diagnósticos, prevenir las enfermedades y prever el riesgo, sostuvo que para alcanzar estos objetivos se requiere de una interacción con ciencia de datos, medición de factores de riesgo, consideraciones clínicas, análisis de estilos de vida y todo lo que transmiten nuestros genes. Adicionalmente, sostuvo que la medicina de precisión va hacia volver la medicina preventiva y salir de que sea netamente reactiva, por esto, la medicina de precisión es el futuro de la medicina

Para finalizar, la panelista ilustró respecto del manejo de datos genéticos y cómo se va a proteger y compartir esa información. Un primer punto importante es la equidad en el acceso, la medicina de precisión es costosa y se tiene que ver cómo se va a hacer para que todas las personas puedan tener acceso equitativo. Por otra parte, está el consentimiento informado ya que es muy importante que la persona sepa que se está interpretando su imagen con ayuda de IA, y debe dar su consentimiento para estos procesos y desde el punto de vista ético-legal, saber que el ser humano es responsable.

Para finalizar, la panelista señaló que la responsabilidad en la toma de decisiones médicas no puede dejar de tomarlas un ser humano, con el apoyo de todos estos estudios y análisis. También mencionó que existen algunos desafíos, por ejemplo, cómo se están gestionando estos datos masivos, ya se están comercializando datos, mencionó que existen los biobancos para estudios, que se pueden vender, pero se debe tener una ética, como tener consentimiento informado entre otros puntos, estos aspectos éticos se deben construir en conjunto de una manera interdisciplinaria, con abogados, filósofos, médicos...etc.

En este punto, el moderador dio paso a Alejandro Rodríguez, quién comenzó su intervención con la precisión de que su intervención presentaría la perspectiva de la industria sobre los desarrollos de IA con responsabilidad y propósito. Sostuvo que los productos que se comercializan deben tener un lineamiento en el desarrollo con un nivel ético y de responsabilidad muy alto.

Seguidamente, expuso tres ejemplos de cómo la IA puede mejorar la experiencia humana en el cuidado de la salud. Por un lado, la IA puede aumentar la experiencia de los proveedores de atención médica y apoyar su toma de decisiones, permitiéndoles hacer lo que mejor saben hacer: detectar, diagnosticar, tratar y monitorear enfermedades. Por otra parte, la IA puede mejorar la eficiencia operativa para ayudar a los proveedores de atención médica a centrarse en la atención al paciente. Y finalmente, la IA puede capacitar a las personas para que cuiden mejor su salud y bienestar al ofrecer información personalizada y procesable que les ayude a desarrollar y mantener hábitos saludables.

Para poder cumplir con las promesas de IA que se ofrece desde la industria, se necesita de tres componentes importantes. Primero los datos, ya que son la fuente principal, se tiene la responsabilidad de informar a los usuarios de donde se obtienen los datos que se van a utilizar para la IA; luego está la gobernanza y la confianza, respecto de la cual indicó que la gobernanza debe ser global, las soluciones que genera la industria no solo sirven en un país sino en todo lado, por lo cual se deben tener esos criterios regulatorios bien definidos.

A continuación, el panelista habló acerca del camino hacia la atención de precisión en el cual, como próxima frontera, la I.A. ayudará a conectar datos de pacientes previamente desconectados y dispares para proporcionar información clave en la toma de decisiones. En la atención del cáncer, por ejemplo, la I.A. puede ayudar a integrar información en diferentes dominios clínicos, como radiología, patología, sistemas de EHR y genómica. Indicó también que, en el futuro, la integración inteligente de los datos podría dar más información sobre el pronóstico, que apoyará la selección de la mejor vía de atención para ese paciente en particular basado en un análisis de los resultados del tratamiento para pacientes similares.

Para finalizar, el panelista compartió los principios en los desarrollos de soluciones de IA de Philips, los cuales son: bienestar, supervisión, robustez, equidad y transparencia.

Como última intervención de esta primera parte del panel, Guillermo Cruz habló acerca de los resultados de un estudio en el que participó en 2021, que revisó prácticas internacionales de aprovechamiento de datos generados por los *wearables*, específicamente relojes, pulseras y demás dispositivos que generan datos asociados a hábitos de salud y documentar los beneficios en salud que se pueden dar a partir del utilizamiento de estos datos y que oportunidades y barreras se tienen en Colombia.

El panelista presentó un resumen de los casos principales de uso de estos datos que se documentaron en ese estudio. La primera tipología fueron los casos de uso, donde los datos se conservan en la esfera del individuo, eventualmente se comparten con el médico del individuo, este es el caso de los relojes que pueden dar información sobre aspectos como monitoreo de tendencias cardio, variables relacionadas con enfermedades como diabetes, tendencias de sueño, número de pasos durante el día...etc. El segundo grupo de casos fue en el que los individuos aceptan compartir esos datos con empresas que pueden ser su empleador o aseguradoras, entrando en un escenario de mayor riesgo a la privacidad, pero se documentaron casos de beneficios al compartir estos datos, por ejemplo empresas que generaron programas de bienestar para sus empleados a partir de la recolección de datos con estos dispositivos, y pusieron metas para mejorar por ejemplo el número de pasos diarios, y a quienes lograran alcanzarlas, les brindaban incentivos. Se documentó que estos programas redujeron gastos en materia de salud de los empleados, reducción en indicadores negativos en salud y aumento en aspectos positivos.

El tercer grupo de casos fueron de Gobiernos que han estado interesados en conocer los datos que generan estos dispositivos, con propósito de promover

mejoras en los hábitos de la población y también, propósitos de investigación científica. Mencionó que en Singapur se diseñó un programa nacional de hábitos saludable con inscripción voluntaria de los ciudadanos para quienes quisieran compartir esa información, quienes lograran avances en los indicadores, podrían recibir beneficios monetarios, también en EE. UU., algunos individuos se inscribieron a un programa en el que compartían su información en un programa de investigación en salud, a cambio, tenían accesos a retroalimentación en salud y hábitos saludables. Estos datos generaron una base importante para investigación en salud.

Respecto a los casos mencionados, el panelista sostuvo que, si bien lograron desarrollos y avances en investigación relacionada con la salud, promoción de buenos hábitos y reducción de gastos en salud, la exposición de estos datos fuera de la esfera del individuo puede tener consecuencias de privacidad y éticas que deben abordarse. En estos casos se dio un manejo de altos estándares éticos y de protección de datos, pero no todos los casos son así y deben revisarse estas implicaciones.

En este punto, el moderador dio paso a las preguntas. Para iniciar, preguntó a Leonardo González que tan importante es el tema ético en el sentido de que la regulación europea prohíbe la recolección de datos biométricos de la cara, pero durante la exposición de los otros panelistas se presentó un caso que parece mucho más importante como la información genética.

El panelista respondió que esto se resuelve desde el contextualismo, es decir, no sólo se debe ver la tipología de los datos sino el contexto para que se requieren, lo que hace que por ejemplo la tensión entre derecho a la intimidad y el derecho a la recolección de datos no se resuelva siempre de la misma manera, sino que se vea siempre al contexto. Dependiendo del contexto donde se encuentre el dato y el tipo de tensión entre derechos de cada caso, tendrá que entrar quien tenga que establecer el juicio y ver qué es lo que se está jugando cuando se tiene acceso a

ese dato. Teniendo en cuenta esto, sostuvo que la recolección y uso de los datos biométricos de la cara, es algo que no debe pasar según lo ha entendido la comisión europea.

Seguidamente, el moderador se dirigió a la Dra. Martha Oyuela para llamar la atención sobre algunos puntos de su presentación, específicamente sobre la posibilidad de alguna manera de predecir la salud de las personas en el transcurso de la vida, y de la equidad en términos de la posibilidad que tengamos todos de acceder a esa tecnología. Con fundamento en eso, preguntó si esto no rayaría con el principio de libertad de las personas, en el sentido de que no a todo el mundo quisiera que le dijeran de que va a sufrir, por tanto, que rol jugaría esa prevención contra la libertad de la persona de tener acceso o no a esa información.

La panelista respondió que se debe ir al principio de autonomía, la beneficencia y la justicia distributiva. Resaltó que obviamente hay un respeto a la autonomía frente a decidir si se quiere participar o no en un estudio de esto, no es una obligación hacerlo, pero el grupo científico si puede ofrecer a la sociedad en general esa posibilidad de que se anticipen a determinar los factores de riesgo que tienen frente al desarrollo de enfermedades y que ellos decidan si quieren o no saberlo y luego proceder. Explicó que en ese punto es muy importante el consentimiento informado donde se le explica a la persona que se le va a realizar, para que sirva, cómo se hace y que así la persona consienta teniendo claro los riesgos que tiene y también los beneficios que se tienen, pero siempre una decisión respetable, personal y autónoma.

Seguidamente, el moderador preguntó a Germán Combariza cuando se está creando una herramienta de IA ¿Cómo se debería hacer para que en ese proceso de elaboración tengan en cuenta cosas como los sesgos, el consentimiento informado, entender cuál puede ser el prejuicio que puede llevar lo que estoy haciendo?

El panelista indicó que cuando llegan los datos, lo que se hace es eliminar toda la información que no interesa para concentrarse en los importantes y a través de estos dar una respuesta. Luego, mencionó que los sesgos vienen una vez está el algoritmo trabajando, dando respuestas, ahí es donde comienza la auditoría del algoritmo y ahí es donde se dan cuenta que el sesgo está fallando, es por eso que es importante que no se deje al algoritmo trabajar sólo, y por eso no va a reemplazar al profesional sino va a ser un asistente, y cuando falle, se necesitará la intervención para dar una retroalimentación del algoritmo.

Frente a la protección de datos, no se suele considerar mucho, ya que se programa a través de números y no se está pensando en que significa el dato para la persona, lo cual puede ser un error, pero se deja esa tarea a la otra persona que está investigando que sabe la importancia de los datos, esa parte corresponde al equipo que es dueño de los datos.

A continuación, el moderador preguntó a Alejandro Rodríguez desde la perspectiva de su empresa ¿Cómo trabajan el tema de no creerle al sistema todo lo que arroja o incluso ir en contra de lo que dice la máquina?

Para responder al interrogante, el panelista en primera medida hizo énfasis en que se debe diferenciar los conceptos de desarrollo, grupos de investigación y productos comercializables. Explicó que los desarrollos van mucho más adelante que los productos que lanza la industria, la razón de esto es que para poder comercializar los productos que tienen una responsabilidad diagnóstica muy alta, se necesitan hacer múltiples etapas de verificación y retroalimentación, y cuando ya está todo verificado y certificado se vuelve producto. Teniendo en cuenta lo anterior, no se comercializan cosas de las que no se tenga la medida seguridad. Agregó también que tienen centros donde se hacen pruebas antes de sacar los productos.

En este punto, la Dra. Martha Oyuela tomó la palabra para observar que siempre que se hace un desarrollo de IA se debe responder a una necesidad. Dijo que es

muy importante para la industria tener una lista de chequeo de preguntas desde el punto de vista ético, para que se pueda responder a unas necesidades y que las personas también puedan conocer cómo se llegó a esa solución, por ejemplo, de donde se construyó la data y si intervinieron profesionales de la salud.

Alejandro Rodríguez respondió a la anterior intervención e indicó que en el caso de Philips si se entrega esa información, pero se debe reconocer que, en la industria, no todo el mundo dice de donde viene la información, lo que compromete un diagnóstico al final. También recalcó la importancia de la transparencia en la entrega de toda la información.

Seguidamente, el moderador preguntó a Guillermo Cruz si las personas que adquieren los denominados Wearables, ¿Realmente saben que recopilan información que puede ser vital y que puede usarse para alimentar herramientas que posteriormente pueden arrojar resultados en temas de salud?

El panelista explicó primero que los Wearables no son dispositivos médicos, pero si generan información valiosa para propósitos de prevención y monitoreo. Indicó que se deben diferenciar dos niveles, por una parte, el manejo de los datos que se da en el dispositivo como tal, y el manejo que se da en el programa de promoción que puede ser implementado por las empresas o gobiernos. En cuanto a los dispositivos, lo que pasa es que tienen unos sensores que captan los datos que son transmitidos al celular y en esa etapa se hace un tratamiento básico y una vez está la información en el teléfono, las marcas de los dispositivos tienen unos servidores que captan esta información donde se hace el procesamiento más elaborado y el análisis retorna al celular y genera graficas e información para el individuo.

Por otra parte, cuando el individuo acepta compartir su información con el gobierno inicia otra fase consistente en que los datos salen del dispositivo y servidor de la marca a un repositorio web que es administrado por la empresa o el gobierno y ahí se requieren otros protocolos de seguridad. En los casos documentados, los

protocolos de seguridad fueron por una parte las políticas de privacidad de los dueños que han sido actualizadas y se ven elementos como el consentimiento para el procedimiento de datos, la transparencia sobre el uso de los datos y el compromiso de no usar los datos para asuntos diferentes a lo especificado ni compartirlos con propósitos comerciales. Adicionalmente tienen practicas de protección de datos como la encriptación.

Para finalizar su intervención, indicó que en estos casos se ve que las empresas o gobiernos han incorporado estas practicas de protección de datos y adicionalmente, teniendo en cuenta que estos programas son voluntarios, el usuario en cualquier momento puede ingresar o salirse del programa, tiene el derecho al olvido, que consiste en que su información se borre de las bases de datos.

A continuación, el moderador preguntó a Germán Combariza, respecto a los objetivos que se trazan al desarrollar un sistema de IA ¿El dato limita frente al objetivo que se quiere en estos programas o es indiferente el dato?

El panelista dijo que normalmente la empresa no sabe lo que quiere, y quien va a hacer el desarrollo debe hacer un primer análisis respecto a lo que se tiene y se quiere, a partir de los datos disponibles, y le da una valoración de si se puede o no lograr lo que quieren y el tiempo que puede costar, pero depende mucho de lo que tenga la empresa, recalcó que es muy importante tomar bien los datos, mencionó como ejemplo cuando se toman datos clínico en papel y eso expone a que hayan muchos errores.

Para cerrar el espacio de preguntas, el moderador preguntó a Leonardo González si ¿Dejar a consideración el tema ético como limite en el uso de estas herramientas es una solución suficiente para limitar, prohibir y marcar los caminos?

El panelista dijo que la respuesta es de complementariedad, porque si bien siempre es necesario un marco normativo estatal, eso no agota toda la normativa de la

acción, siempre van a quedar vacíos en acciones y micro acciones, y es ahí donde la ética tiene su campo, entonces no es que una reemplace a la otra, sino que se necesita una complementariedad, por ejemplo, el estado reglamenta, pero el que la usa es la persona, por eso también se requiere un uso ético, que es un tema personal. Por otra parte, dijo que se debe suponer la libertad y la agencia del ser humano, pero a nivel estatal queda en entredicho las posibilidades de acción que se tienen por parte de las personas, pero que él está totalmente a favor de la complementariedad entre ambos ámbitos.

El moderador cerró el panel agradeciendo la intervención a los panelistas, a los organizadores y a todos los participantes, indicó que el tema tratado es de gran interés y que se van a seguir dando este tipo de discusiones tan valiosas. Además, se invitó a seguir las próximas convocatorias a eventos y publicaciones del Departamento de Derecho, Comunicaciones y Tecnologías de la Información.