ISSN: 2215-3276

ÉTICA JUDICIAL

CUADERNO 24

Vol. 13, n.° 2, enero-junio 2024

CIEJ
Comisión Iberoamericana de Ética Judicial

PODER JUDICIAL
República de Costa Rica

CONSEJO ASESOR ÉTICA JUDICIAL
PODER JUDICIAL

Ética Judicial
Cuaderno 24
enero- junio 2024

ISSN
2215-3276

Coordinador de la publicación: Rafael León Hernández
Diseño de portada y diagramación: Mónica Cruz Rosas
Corrección filológica: Área de Servicios Técnicos, Escuela Judicial
Los dictámenes de la Comisión Iberoamericana de Ética Judicial no han sido revisados en virtud de que son reproducciones literales de dictámenes aprobados

http://eticayvalores.poder-judicial.go.cr/
http://www.poderjudicial.es/cgpj/es/CIEJ

Contenido

USO ÉTICO DE LA INTELIGENCIA ARTIFICIAL EN LA LABOR JURISDICCIONAL

PONENTE: LUIS PORFIRIO SÁNCHEZ RODRÍGUEZ

VIGESIMOCUARTO DICTAMEN, DE 8 DE SEPTIEMBRE DE 2023, DE LA COMISIÓN IBEROAMERICANA DE ÉTICA JUDICIAL

I. La preocupación ética por el uso de la inteligencia artificial en la justicia

1. En 2020 Comisión Iberoamericana de Ética Judicial tuvo ocasión de explorar en su *Noveno dictamen sobre el uso por el juez de las nuevas tecnologías,* el empleo de la Inteligencia Artificial (IA) en el ejercicio de la función de juzgar. Nuestro dictamen señala la importancia de velar por los derechos humanos y enuncia diversos principios éticos al hacer uso de la IA, haciéndose eco de algunos referentes como la *Declaración sobre ética y protección de datos en el sector de la inteligencia artificial* aprobada en 2018 por las autoridades de protección de datos de la Unión Europea y el *Libro blanco sobre la inteligencia artificia*l de 2020 de la Comisión Europea.

2. El *Dictamen* de la Comisión retomaba, específicamente y respecto de la administración de justicia, los principios contenidos en la *Carta Ética Europea sobre el uso de la inteligencia artificial,* aprobada en 2018 por la Comisión Europea para la Eficiencia de la Justicia (CEPEJ), del Consejo de Europa. También resaltaba la repercusión que había tenido en diversos tribunales el uso de algoritmos en el ámbito penal y administrativo, relativos al tratamiento privado de los datos, su interpretación y los fines perseguidos, así como la posibilidad de que se exacerbasen los sesgos ya presentes en los datos. Y, en fin, reconocía las ventajas que representaba el uso de la IA en la optimización de tareas rutinarias y de orden cuantitativo, reservando a las personas juzgadoras la adopción de las decisiones judiciales.

3. En 2021, en el marco de las Naciones Unidas, la UNESCO adoptó la *Recomendación sobre la ética de la inteligencia artificial*, que propone valores y principios que buscan, entre otras cuestiones, orientar a los Estados en la formulación de leyes, políticas u otros instrumentos relativos a la IA y las acciones para asegurar la incorporación de la ética en todas las etapas del ciclo de vida de los sistemas de IA[1].

1 UNESCO (2021). Recomendación, de 23 de noviembre de 2021, sobre la ética de la inteligencia artificial, París.

4. Esta *Recomendación* enumera unos valores como son: 1) Respeto, protección y promoción de los derechos humanos, las libertades fundamentales y la dignidad humana 2) Prosperidad del medio ambiente y los ecosistemas 3) Garantizar la diversidad y la inclusión 4) Vivir en sociedades pacíficas, justas e interconectadas.

5. La misma *Recomendación* enuncia los principios en los que se inspira: 1) Proporcionalidad e inocuidad 2) Seguridad y protección 3) Equidad y no discriminación 4) Sostenibilidad, 5) Derecho a la intimidad y protección de datos 6) Supervisión y decisión humanas 7) Transparencia y explicabilidad 8) Responsabilidad y rendición de cuentas 9) Sensibilización y educación 10) Gobernanza y colaboración adaptativas y de múltiples partes interesadas.

6. En relación con el poder judicial, la *Recomendación* de la UNESCO señala la necesidad de prever mecanismos para vigilar el impacto social y económico de dichos sistemas y el deber de los Estados de reforzar la capacidad del Poder Judicial para adoptar decisiones relacionadas con IA, particularmente en lo relativo a la protección de los derechos humanos, el estado de derecho, la independencia judicial y el principio de supervisión humana, así como la fiabilidad de esos sistemas, su orientación al interés público y centrados en el ser humano.

7. En 2022 la Organización para la Cooperación y el Desarrollo Económicos (OCDE) elaboró un estudio sobre el *Uso estratégico y responsable de la inteligencia artificial en el sector público de América Latina y el Caribe*, en el que recomienda la aplicación de los Principios de la OCDE sobre IA y el desarrollo de marcos éticos a nivel nacional[2]. Los principios propuestos por la OCDE son: 1) Crecimiento inclusivo, desarrollo sostenible y bienestar 2) Valores y equidad centrados en el ser humano 3) Transparencia y explicabilidad 4) Robustez, seguridad y protección 5) Responsabilidad[3].

---

2 OECD/CAF (2022), *Uso estratégico y responsable de la inteligencia artificial en el sector público de América Latina y el Caribe,* Estudios de la OCDE sobre Gobernanza Pública, OECD Publishing, París, https://doi.org/10.1787/5b189cb4-es.

3 OCDE (2019). Recomendación, de 22 de mayo de 2019, del Consejo sobre Inteligencia Artificial, OECD/LEGAL/0449.

8. En 2023 la Unión Europea está en un proceso avanzado de adopción de una *Ley de Inteligencia Artificial* donde, en particular, considera "de alto riesgo ciertos sistemas de IA destinados a la administración de justicia y los procesos democráticos, dado que pueden tener efectos potencialmente importantes para la democracia, el Estado de Derecho, las libertades individuales y el derecho a la tutela judicial efectiva y a un juez imparcial. En particular, a fin de evitar el riesgo de posibles sesgos, errores y opacidades, procede considerar de alto riesgo aquellos sistemas de IA cuyo objetivo es ayudar a las autoridades judiciales a investigar e interpretar los hechos y el Derecho y a aplicar la ley a unos hechos concretos. No obstante, dicha clasificación no debe hacerse extensiva a los sistemas de IA destinados a actividades administrativas meramente accesorias que no afectan a la administración de justicia en casos concretos, como la anonimización o seudonimización de las resoluciones judiciales, documentos o datos; la comunicación entre los miembros del personal; tareas administrativas, o la asignación de recursos"[4]. En una de sus enmiendas, el Parlamento Europeo ha establecido límites al uso de la IA en el ámbito judicial y a modo de principio ha proclamado: «La utilización de herramientas de inteligencia artificial puede apoyar la toma de decisiones, pero no debe substituir el poder de toma de decisiones de los jueces o la independencia judicial, puesto que la toma de decisiones finales debe seguir siendo una actividad y una decisión de origen humano»[5].

9. Pues bien, en este contexto en la XVIII reunión de la Comisión Iberoamericana de Ética Judicial, celebrada en Santo Domingo, República Dominicana, los días 20 y 21 de febrero de 2023, considerando los avances e incorporación de nuevas tecnologías en los poderes judiciales, se acordó la realización de un nuevo dictamen relativo específicamente a la IA y a su uso en la labor jurisdiccional desde una perspectiva ética.

---

4 Comisión Europea, *Propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se establecen normas armonizadas en materia de inteligencia artificial (ley de inteligencia artificial)* y se modifican determinados actos legislativos de la Unión, COM/2021/206 final, Bruselas, 21 de abril de 2021.

5 Parlamento Europeo, *Enmiendas aprobadas por el Parlamento Europeo el 14 de junio de 2023 sobre la propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se establecen normas armonizadas en materia de inteligencia artificial (Ley de Inteligencia Artificial) y se modifican determinados actos legislativos de la Unión* (COM(2021)0206 – C9-0146/2021 – 2021/0106(COD)), P9_TA(2023)0236, A9-0188/2023.

II. La inteligencia artificial y su uso en el ejercicio de la función jurisdiccional

10. La Inteligencia Artificial (IA) es el resultado del desarrollo de sistemas informáticos computacionales que simulan o pueden realizar tareas que normalmente requieren inteligencia humana, como la percepción, el razonamiento y el aprendizaje.

11. En el ámbito judicial, la IA puede ser utilizada, por ejemplo, para la automatización y mejora de los procesos, como pueden ser la identificación y comparación de pruebas, verificación y compilación de datos, programación de audiencias. Todas estas tareas pretenden una reducción de las cargas de trabajo de las personas juzgadoras y una reducción en los tiempos de tramitación de los casos. Ahora bien, la IA también puede ser utilizada en labores más sustanciales como la toma de decisiones, la predicción de resultados y hasta la determinación de probabilidades de que una persona pueda volver a delinquir; lo que genera cuestionamientos éticos sobre la conveniencia o mejor forma de uso.

12. La excesiva litigiosidad y cargas de trabajo justifican el uso de la IA como un instrumento que permita reducir la mora judicial y la duración de los procesos, contribuyendo a la meta de contar con una justicia pronta y cumplida.

13. La capacidad de la IA ha crecido exponencialmente en los últimos años, permitiendo que, entre sus numerosas funciones, pueda comprender e interpretar el lenguaje humano en diversas lenguas, analizar y comparar grandes cantidades de datos, identificar patrones y tendencias y, en lo relativo a temas de nuestro interés judicial, hasta comparar e interpretar determinadas regulaciones para aplicarlas a casos concretos.

14. En algunos países han comenzado a usar la IA para la resolución de casos de menor cuantía con el fin de reducir la mora judicial, como es el caso de Estonia[6] y China[7], pero limitándose a tareas sencillas como el cotejo de pruebas o verificación de la información, reservándose la resolución a jueces humanos, aunque este tipo de sistemas ya son capaces de "sugerir" la resolución de los casos.

6 The Technolawgist (2019). *Estonia se prepara para tener "jueces robot" basados en inteligencia artificial.*

7 Zhabina, A. (2023). Las cortes de China ya utilizan inteligencia artificial para resolver casos.

15. La IA también se utiliza en los ámbitos judiciales para predecir el comportamiento delictivo de una persona, por ejemplo, sus probabilidades de reincidencia y, por tanto, influye directa o indirectamente en la determinación de las sentencias que dictan las personas juzgadoras[8].

16. Los sistemas de IA también se emplean en Iberoamérica, por ejemplo, en Argentina donde el programa Prometea se usa para la redacción de documentos y para la automatización de tareas de varias organizaciones, en un proyecto iniciado por la Fiscalía General Adjunta en lo Contencioso Administrativo y Tributario del Ministerio Público Fiscal de la Ciudad de Buenos Aires, pero que se ha extendido a otras organizaciones[9].

17. En Costa Rica, se ha logrado desarrollar tres proyectos de los cuales dos ya se encuentran en una fase productiva, que son el tipificador de documentos que permite clasificar los escritos presentados en los despachos de cobro, de forma automática y el chat bot, que permite responder preguntas sobre temas del Poder Judicial y datos de la consulta pública de los expedientes de cobros. La última solución que se encuentra en una fase de pruebas es un transcriptor de voz a texto.

18. Por otro lado, algunas personas juzgadoras, por iniciativa propia y sin que existan regulaciones al respecto, están utilizando sistemas de IA de uso público para la redacción de sus propias resoluciones o la revisión de jurisprudencia.

19. Paralelamente, las personas litigantes pueden aprovechar la IA para determinar tendencias en relación con las valoraciones o decisiones de una persona juzgadora, por ejemplo, a qué pruebas o clase de testigos suele la persona juzgadora dar más crédito (si es proclive a confiar en peritos de un área específica), lo que les daría, a la vista de estos parámetros, la posibilidad de definir su estrategia procesal.

---

8 Maybin, S. (2016). *¿Cómo en Estados Unidos las matemáticas te pueden meter en prisión?,* BBC News.

9 Ministerio Público Fiscal (2022). *Innovación e Inteligencia Artificial,* Buenos Aires, Argentina.

20. En 2020 en Brasil el Consejo Nacional de Justicia adoptó una Resolución sobre la ética, la transparencia y la gobernanza en la producción y en el uso de Inteligencia Artificial en el Poder Judicial[10]. A tal efecto, el Poder Judicial brasileño ha creado la plataforma *Sinapses* que define como "solución informática, mantenida por el Consejo Nacional de Justicia, cuyo objetivo es almacenar, probar, entrenar, distribuir y auditar modelos de Inteligencia Artificial". En la misma Resolución se han adoptado unas normas muy detalladas cuyo fin es garantizar el respeto de los derechos fundamentales, en particular prohíbe la discriminación, facilita la publicidad y la transparencia, promueve la gobernanza y la calidad, refuerza la seguridad, posibilita el control del usuario y garantiza la rendición de cuentas y la responsabilidad de toda solución informática que utilice modelos de IA.

III. Las oportunidades y los retos en el uso de la Inteligencia Artificial en el ejercicio de la función judicial

21. En el ámbito judicial, la IA muestra múltiples oportunidades de uso que podrían facilitar las labores, minimizar los errores y disminuir la duración de los procesos, pero también constituye un reto en otros ámbitos que invitan a su uso con la máxima cautela.

22. Por una parte y en cuanto a las oportunidades, con la IA es posible automatizar tareas rutinarias y repetitivas como la programación de audiencias, la revisión y archivo de expedientes o la selección de jurisprudencia, lo que puede ahorrar tiempo y recursos humanos dedicados a estas tareas.

23. También el uso de la IA consigue mejorar la valoración e interpretación de la prueba, como, por ejemplo, en la revisión de registros telefónicos, correos electrónicos o mensajes de texto, donde se pueden identificar sus patrones, frecuencias y relaciones.

24. Asimismo, la IA logra señalar detalles en audios, fotografías y videos que podrían pasar desapercibidos para un observador humano. En este orden de ideas, puede utilizarse en el análisis de ADN, en la identificación de huellas dactilares y en la interpretación de imágenes médicas.

---

10 Brasil. Consejo Nacional de Justicia, Resolución nº 332, de 21 de agosto de 2020 sobre la ética, la transparencia y la gobernanza en la producción y en el uso de Inteligencia Artificial en el Poder Judicial, Brasilia.

25. La capacidad de proceso de información facilitaría que la IA realice análisis de grandes conjuntos de sentencias para determinar patrones o prejuicios relativos a temas como sexo, género, nacionalidad, entre otros, lo que ayudaría a minimizar su efecto en sentencias futuras.

26. De igual forma, puede ser utilizada para resolver consultas legales de forma inmediata y gratuita, por ejemplo, explicando los alcances de una norma o los requisitos para iniciar algún tipo de proceso, lo que aportaría equidad en el acceso a la justicia para personas que no poseen ingresos suficientes para costear su asistencia legal.

27. En cambio, la IA presenta soluciones con las que se debe tener la mayor cautela: la primera es su capacidad para analizar el lenguaje verbal y gestual de las personas para interpretar si éstas son sinceras o mienten; la segunda tiene que ver con la predicción de las probabilidades de que una persona delinca (o lo vuelva a hacer) en el futuro, como un insumo para los jueces y juezas a la hora de dictar sentencia; y, en tercer lugar, la IA es capaz de analizar toda la prueba disponible y sugerir (o dictar) una sentencia, sin necesidad de un juez humano.

28. A la vista de las potencialidades de la IA podemos percibir algunos de sus riesgos y limitaciones. De hecho, la regulación de la Unión Europea que está en proceso de adopción en 2023 pretende clasificar los sistemas de IA de Asuntos relacionados con la aplicación de la ley y de la Administración de Justicia como de alto riesgo[11].

11 En el Anexo de la futura *Ley de Inteligencia Artificial de la Unión Europea*, ante citada, se recogen, por una parte, en el epígrafe Asuntos relacionados con la aplicación de la ley los siguientes supuestos calificados de alto riesgo: "a) sistemas de IA destinados a utilizarse por parte de las autoridades encargadas de la aplicación de la ley para llevar a cabo evaluaciones de riesgos individuales de personas físicas con el objetivo de determinar el riesgo de que cometan infracciones penales o reincidan en su comisión, así como el riesgo para las potenciales víctimas de delitos; b) sistemas de IA destinados a utilizarse por parte de las autoridades encargadas de la aplicación de la ley como polígrafos y herramientas similares, o para detectar el estado emocional de una persona física; c) sistemas de IA destinados a utilizarse por parte de las autoridades encargadas de la aplicación de la ley para detectar ultrafalsificaciones a las que hace referencia el artículo 52, apartado 3; d) sistemas de IA destinados a utilizarse por parte de las autoridades encargadas de la

29. En primer lugar, como cualquier sistema informático, es susceptible de sufrir ataques de *hackers*, virus, como los troyanos, o procedimientos similares, lo que podría vulnerar cualquier garantía probatoria, los datos personales o los archivos judiciales que estén siendo procesados por la IA.

30. Al menos en los primeros momentos de implementación de tecnologías que utilicen IA, parte de la ciudadanía puede ser reticente o desconfiar de la fiabilidad o conveniencia de su uso.

31. En numerosos casos, las tecnologías más avanzadas son desarrolladas por entidades privadas o externas a los Poderes judiciales, que podrían tener otro tipo de intereses, posiblemente más económicos que sociales, en el uso de los datos. Por lo general, las instituciones públicas no cuentan con personal profesional y técnico para conocer la forma en que operan estos sistemas, lo que genera una gran dependencia de proveedores externos.

32. El uso de la IA afecta a la garantía de determinados derechos fundamentales de gran trascendencia en una sociedad democrática: la intimidad, la privacidad y la protección de los datos personales, lo que constituye un particular reto frente a la introducción de sistemas de IA, porque el procesamiento de la información de las causas judiciales podría llevarse a cabo mediante sistemas informáticos

---

aplicación de la ley para la evaluación de la fiabilidad de las pruebas durante la investigación o el enjuiciamiento de infracciones penales; e) sistemas de IA destinados a utilizarse por parte de las autoridades encargadas de la aplicación de la ley para predecir la frecuencia o reiteración de una infracción penal real o potencial con base en la elaboración de perfiles de personas físicas, de conformidad con lo dispuesto en el artículo 3, apartado 4, de la Directiva (UE) 2016/680, o en la evaluación de rasgos y características de la personalidad o conductas delictivas pasadas de personas físicas o grupos; f) sistemas de IA destinados a utilizarse por parte de las autoridades encargadas de la aplicación de la ley para la elaboración de perfiles de personas físicas, de conformidad con lo dispuesto en el artículo 3, apartado 4, de la Directiva (UE) 2016/680, durante la detección, la investigación o el enjuiciamiento de infracciones penales; g) sistemas de IA destinados a utilizarse para llevar a cabo análisis sobre infracciones penales en relación con personas físicas que permitan a las autoridades encargadas de la aplicación de la ley examinar grandes conjuntos de datos complejos vinculados y no vinculados, disponibles en diferentes fuentes o formatos, para detectar modelos desconocidos o descubrir relaciones ocultas en los datos". Y, por otra parte, bajo el epígrafe Administración de justicia y procesos democráticos se refiere a estas actividades de alto riesgo: "a) sistemas de IA destinados a ayudar a una autoridad judicial en la investigación e interpretación de hechos y de la ley, así como en la aplicación de la ley a un conjunto concreto de hechos".

desarrollados, operados y/o pertenecientes a empresas privadas, tanto locales como multinacionales, sobre los cuales el Estado podría ejercer un bajo o un nulo control directo. Esto conduce a la necesidad de establecer pautas claras para el tratamiento de los datos y mecanismos de fiscalización. También dentro de cada Estado puede producirse un reparto de competencias en cuestiones tecnológicas que asuma los respectivos Ministerios de Justicia y que no deberían impedir el pleno control judicial sobre estas cuestiones.

33. Debido a condiciones inherentes a la informática en su estado actual, se manifiestan problemas particulares para garantizar la transparencia y explicabilidad de las decisiones judiciales tomadas con ayuda o a través de la IA. El código de programación suele ser una parte sensible de todo programa informático, en primer lugar, por las implicaciones de propiedad intelectual (tanto si el sistema lo desarrollan empresas privadas, comprado a una de estas, o desarrollado a lo interno del sistema judicial). Con independencia de lo anterior, si el sistema es de acceso libre (código abierto, en general, o acceso privativo para las partes) o se encuentra en redes, esto lo hace más vulnerable a ataques informáticos, tanto para influir en el caso concreto o el funcionamiento general del sistema, como para perpetrar ataques contra las instituciones o la estabilidad de los Estados.

34. En todo caso los programas que utilizan IA no son infalibles, por lo que pueden dar información errónea que sería asumida como verdadera sin mayor cuestionamiento por los usuarios finales que pueden acostumbrarse a confiar ciegamente en los resultados que presenten estos sistemas, o bien, sin posibilidad de contrastarlos con otras fuentes que permitan verificar la información.

35. Los programas de IA utilizan como materia prima la información estadística que recopilan de fuentes, hasta ahora, manejadas por seres humanos; esto implica que, si la información base presenta algún tipo de sesgo, la IA podrá reproducirlos e, incluso, acrecentarlos. Por ejemplo, si en un país son frecuentes los arrestos

de los ciudadanos de una población minoritaria, como sucede en muchas ocasiones con los migrantes, los programas podrían interpretar que las personas migrantes, en general, tienen mayor tendencia a delinquir, cuando puede ser que esto n

36. Por medio de la IA también sería posible la fabricación de pruebas. Por ejemplo, ya se está utilizando para la creación de fotografías y videos donde aparecen personas que realmente no estuvieron presentes. También es posible la simulación de voces o la réplica de estilos y rasgos de escritura, lo que dificulta distinguir entre las pruebas artificiosas y las reales.

37. La determinación de responsabilidades es otro factor a considerar, así, por ejemplo, si un sistema de IA realiza un análisis incorrecto o toma una decisión equivocada que oriente en un sentido determinado la resolución judicial, sería difícil determinar quién es el responsable de ese error, pudiendo ser las personas que lo diseñaron, las que le ingresaron la información, quien se basó en sus resultados para decidir o, incluso, cabe la posibilidad de que se determine que la responsabilidad sea debida, en exclusiva, a un error del sistema.

38. Pese a que el uso de tecnologías ha permitido que el acceso a la justicia llegue a más personas, tampoco se puede ignorar que hay otras con poco o nulo acceso a ella, ya sea por factores geográficos, económicos y hasta generacionales, que tienen dificultades de acceso a las tecnologías, lo que también ocurre con IA.

39. El desarrollo de la IA se ha acelerado en los últimos años, mientras que las regulaciones sobre su uso son apenas incipientes en la mayoría de los países. Es más, la adaptación normativa no es capaz de seguir el ritmo del actual crecimiento tecnológico, generando vacíos en relación con las acciones que se puedan realizar, tanto desde una estrategia preventiva como de otra estrategia de control y sanción para los usos indebidos.

40. En suma y en el mundo actual la IA carece de capacidad de juicio moral, por lo que no puede comprender el contexto emocional o psicológico de una situación concreta o bien no puede interpretar a ciencia cierta el espíritu de las normas, lo que es esencial para la labor jurisdiccional, por ejemplo, en el manejo del margen de discrecionalidad inherente en la adopción de una decisión judicial.

IV. Los aspectos éticos del uso de la inteligencia artificial a la luz del Código Iberoamericano de Ética Judicial

41. Si bien el Código Iberoamericano de Ética Judicial (CIEJ) no menciona directamente la IA, sus principios y virtudes deben aplicarse al uso de este tipo de tecnologías en la labor jurisdiccional.

42. La más reciente propuesta de actualización del Código Iberoamericano de Ética Judicial, pendiente de su aprobación por la Cumbre Judicial Iberoamericana, pretende que un nuevo artículo *82quinquies*, referido precisamente a las nuevas tecnologías, resalte la importancia de su uso en el ejercicio de la función judicial y reconozca los límites impuestos por los derechos fundamentales de la persona.

43. Los artículos 1 al 8 del Código reiteran la importancia de la independencia de los jueces, tanto en relación con factores externos como entre pares. Si la IA sustituyera plenamente las decisiones humanas en el análisis jurídico y probatorio de casos concretos se desnaturalizaría el sistema judicial de inspiración democrática, basado en la confianza de la sociedad en sus personas juzgadoras, que son llamadas a resolver litigios de manera independiente. El criterio humano es imprescindible ante discusiones jurídicas novedosas que presenten zonas grises, frente a las cuales la diversidad de opiniones (según los distintos contextos, formación, ideología jurídica y métodos de razonamiento) permite mantener la función judicial como un instrumento vivo, que evoluciona y se adapta a las necesidades de la sociedad.

44. El artículo 9 del CIEJ señala la importancia de la imparcialidad fundada en el derecho objetivo de los justiciables a ser tratados por igual, lo que implica que las decisiones judiciales no deben verse afectadas por prejuicios y estereotipos, lo que es relevante en el uso de la IA, en la medida en que los algoritmos pueden aplicar sesgos que se encuentren ya inmersos en los datos de los cuales se valen las nuevas tecnologías para tomar sus decisiones.

45. La obligación ética de la motivación y, más en particular, las obligaciones que impone el artículo 23 del Código al juez exigen, ante las avanzadas capacidades de la IA para alterar e, incluso, falsificar o generar material textual y audiovisual de gran verosimilitud, que se tenga especial cuidado en la admisión y en la valoración probatoria donde se empleen herramientas tecnológicas tradicionales o incluso las basadas en la misma IA.

46. El vertiginoso desarrollo de las tecnologías impone, a la luz de los artículos 28 a 34 del Código, una adquisición de conocimientos técnicos de las personas juzgadoras y del personal de apoyo a la función judicial y una capacitación constante.

47. En relación con los principios de Justicia y Equidad, enunciados en los artículos del 35 al 40 del Código, el sistema judicial se enfrenta al reto de velar por que el acceso o el posible uso de la IA no confiera ventajas indebidas a las partes en los procesos judiciales, en la medida en que no todas las personas tienen el mismo acceso a las tecnologías.

48. Dada la alta complejidad de las tecnologías empleadas por la IA, existe el riesgo de profundizar las brechas existentes entre el sistema de justicia y la población. El lenguaje jurídico es complejo por sí mismo, al punto de que se exige la asesoría de profesionales en derecho en muchos procesos judiciales. Si a ello se suma la necesidad de comprender el lenguaje informático en que se funda la IA, se genera otro nivel de separación, con conocimiento técnico ajeno a una amplia mayoría de las personas. Inclusive, la gran mayoría de los operadores jurídicos actuales tiene nociones básicas sobre el funcionamiento de la IA por lo que se requiere una preparación profesional para adquirir las competencias necesarias para entender su funcionamiento y para evaluar sus mecanismos y apuntar cuestionamientos en un caso concreto.

49. A la vista de la responsabilidad institucional consagrada por el artículo 42 del Código, el juez es responsable de verificar el buen funcionamiento de todo el sistema judicial por lo que está obligado y queda comprometido a comprobar el adecuado uso que se dé a los sistemas de IA que se implementen en el Poder Judicial. Esta responsabilidad, según el artículo 41 del Código, debe considerarse en relación con la persona juzgadora como individuo y desde el punto de vista institucional, lo cual se extiende a la toma de decisiones sobre qué mecanismos de la IA procedería implementar.

50. El principio de transparencia, enunciado por el artículo 57 del Código, señala la responsabilidad del juez y, por ende, de todo el sistema judicial, de ofrecer información útil, pertinente, comprensible y fiable. Esta responsabilidad compromete el manejo de la prueba y la revisión documental que se pueda realizar por medio de la IA, ya que las personas justiciables tienen que comprender la forma en que se maneja esa información para poder confiar en la veracidad de los datos que por medio de ella se obtengan.

V. Las recomendaciones para un uso ético de la inteligencia artificial en el ámbito judicial

51. La implementación de los sistemas de IA puede mejorar la eficiencia y ser de ayuda en los procesos judiciales. No obstante, debe mantenerse la supervisión o revisión humana para prevenir cualquier funcionamiento indebido o desviado que pueda afectar a la adecuada prestación del servicio judicial.

52. La utilización de la IA para predecir la reincidencia debería descartarse. En todo caso, no es prudente que las personas juzgadoras se dejen influir por este tipo de proyecciones a la hora de emitir sus sentencias, ya que estas deben estar orientadas por la legislación y la valoración fáctica de cada caso concreto, no por proyecciones que pueden o no realizarse.

53. A juicio de la Comisión, la IA puede colaborar en múltiples tareas dentro del sistema judicial, pero la labor de juzgar y de adoptar decisiones judiciales debe seguir siendo una función propia de las personas juzgadoras, que deben tener la capacidad de comprender el espíritu de las normas y las implicaciones de cada caso concreto y que, al mismo tiempo, deben responder por sus decisiones.

54. En el momento tecnológico actual y para la utilización de sistemas de IA en el ámbito jurisdiccional se recomienda no encomendar a la IA razonamientos complejos ni el ejercicio de técnicas de ponderación en las decisiones judiciales sino tareas repetitivas que generen patrones de un mismo comportamiento y que así generen predicciones

tanto en el funcionamiento como en la clasificación de gestiones, el cumplimiento de requisitos, la cumplimentación de formularios y otras tareas de similar naturaleza.

55. Los Poderes judiciales deben procurar que los sistemas de IA que utilicen sean transparentes y comprensibles para las personas juzgadoras y para la ciudadanía. Los trámites y decisiones que utilicen la IA deben ser rastreables y explicables para garantizar la confianza de los ciudadanos en los procesos judiciales.

56. Como parte del deber de transparencia de la Administración Pública, los desarrollos de la inteligencia artificial deben basarse en algoritmos de "cajas blancas", que eviten la opacidad, es decir deben guiarse por la explicabilidad y deben permitir la trazabilidad, lo que implica que a la persona usuaria se le informe y sepa cuándo interactúa con un sistema de IA. Por esa misma razón, para un servicio público de justicia en una sociedad democrática no se recomiendan los sistemas de "cajas negras", es decir aquellos en los que se incluyen datos de los que no se conoce su procesamiento.

57. Deben aprobarse programas de capacitación para jueces, juezas y demás personal relacionado con la administración de justicia sobre el uso y las responsabilidades que genera la implementación de la IA. Es esencial que tales programas de capacitación tengan en cuenta la dimensión ética del uso de la IA.

58. Se recomienda promover una cultura, una capacitación y una sensibilización del personal judicial sobre los conceptos, funcionamiento y apoyo de los ambientes y sistemas de IA en las labores cotidianas, enfatizando en el uso de estas herramientas para tareas repetitivas y de menor complejidad, para así dedicar al personal a las tareas más complejas. Para ello, es clave insistir, como hacen las *Normas Éticas Sobre Inteligencia Artificial* de la OCDE (2019) y de

la UNESCO (2021), en la necesidad de colocar al ser humano como el centro y fin de la IA, evitando así los mitos y los temores sobre los desplazamientos y despidos de personal por la utilización de estas nuevas herramientas. Estos mitos y creencias impiden el desarrollo cuando, en realidad, es el personal judicial quien debe encargarse de entrenar y alimentar con datos estos sistemas y ambientes de IA.

59. Es conveniente que, a la hora de regular el uso de la IA, los Poderes Judiciales de Iberoamérica tengan en cuenta los desarrollos habidos en los organismos internacionales como la UNESCO, la OCDE o en otros ámbitos supranacionales, como la Unión Europea. Estas políticas incluirían principios de ética aplicada con el objetivo principal de tener al ser humano como la referencia de tales herramientas, evitando la discriminación, sesgada o por ruido, en la programación, aplicando los principios de inocuidad y proporcionalidad de tal modo que sus desarrollos se utilicen únicamente para el fin por el cual fueron creados, y regulando con carácter restrictivo los altos riesgos y la vulneración de los datos personales sensibles, por ejemplo, en lo que a la identificación biométrica se refiere. Estas políticas deberán adaptarse a una Estrategia Nacional de Inteligencia Artificial con el fin de evitar contradicciones en el servicio público y de gobierno digital.

60. Con el objetivo de garantizar la innovación y el desarrollo, pero, al mismo tiempo, proteger los datos sensibles y restringidos de las personas usuarias, las políticas referidas a la IA que se formulen deberán incorporar reglas sobre protección y supresión de datos que no limiten el funcionamiento de los sistemas. Para ello, se recomienda diseñar estrategias adecuadas de gobernanza de datos que equilibren la supresión con la alimentación y entrenamiento de los sistemas, pues sin datos, difícilmente se generarán nuevos desarrollos tecnológicos.

61. Es importante el monitoreo de los sistemas de IA para verificar que no estén replicando o aumentando sesgos ya presentes en las bases de datos originales; de igual forma, deben establecerse sistemas de control y vigilancia informática para prevenir cualquier tipo de vulneración externa, facilitando la detención de hackers y de otros intrusos que puedan intervenir ilegítimamente en las bases de datos y pudiendo de ese modo desnaturalizar sus resultados.

62. Es muy recomendable crear equipos de revisión o auditoría externos a los equipos de desarrollo, integrados por desarrolladores informáticos, científicos de datos, profesionales jurídicos que sean especialistas en Derecho informático e IA, así como especialistas en Ética aplicada con el fin de evaluar, sin conflicto de interés, los desarrollos de IA en temas de protección de datos, sesgos éticos y algorítmicos, apego al principio de legalidad y al derecho fundamental de acceso a la justicia, cuyas recomendaciones sean vinculantes a los procesos de desarrollo.

63. Los principios de imparcialidad, justicia y equidad, responsabilidad institucional y transparencia, tal como se proclaman en el Código Iberoamericano de Ética Judicial, deben tenerse en cuenta a la hora de velar por la garantía y el respeto del debido proceso en el uso de la IA en el ejercicio de la función judicial.

64. En todo caso, sea quien tenga las competencias dentro de cada Estado de proporcionar las tecnologías y los sistemas de información que utilice por la Administración de Justicia, estos deberán someterse al control y a la garantía del poder judicial, de modo que el control último no esté en manos de los técnicos sino que corresponda a los jueces.

LAS EXIGENCIAS ÉTICAS FRENTE A UN EXCESO EN LA INVOCACIÓN DE INHABILIDADES PARA JUZGAR

PONENTE: JUSTINIANO MONTERO MONTERO

VIGESIMOQUINTO DICTAMEN, DE 8 DE SEPTIEMBRE DE 2023, DE LA COMISIÓN IBEROAMERICANA DE ÉTICA JUDICIAL

I. Introducción

1. En los procesos judiciales las partes son beneficiarias de un conjunto de garantías que aseguran el comportamiento adecuado de las personas intervinientes en la impartición de justicia, entre las que se encuentra la denominada recusación como un mecanismo institucional puesto a la disposición de los justiciables para utilizarlo cuando exista el riesgo del incumplimiento del principio de imparcialidad, vinculado indisolublemente, a los de igualdad y equidad que los jueces deben respetar en su actuación.

2. La inhibición se asocia comúnmente al reconocimiento de que en el juez concurre una causa de recusación, aunque, en no pocas ocasiones, se advierten prácticas procesales impropias que consisten en construir causas de recusación artificiales, seguidas de solicitudes de inhibición, lesivas de la imagen de los integrantes de un tribunal determinado y hasta de la propia judicatura.

3. Como derecho fundamental de los jueces, la inhibición actúa a favor de los justiciables en la salvaguarda y protección de la transparencia como uno de los ejes que configura la imparcialidad, porque de no declararse su existencia pudiera dar paso a la interposición de la recusación con el fin de apartar al juez del conocimiento del proceso, conducta que se concreta en un comportamiento ético susceptible de cuestionamiento fundado.

4. La recusación y la inhibición conciernen a situaciones vinculadas estrechamente con la garantía de la imparcialidad; mientras la recusación es una prerrogativa procesal impulsada por la parte interesada, la inhibición es una manifestación que proviene del juez, la cual en su contenido esencial reviste, además de un componente procesal, una carga ética significativa.

5. La inhibición, ya sea en forma individual o colectiva, no debe utilizarse para rehusar la responsabilidad de juzgar en un contexto social, influenciado en ocasiones por la presión mediática de sectores defensores de sus propios intereses, o de profesionales que usan el arma de la temeridad como forma de amedrentamiento por lo que atañe a la judicatura que debe estar a la altura de los principios y valores, que constituyen su razón de ser.

6. La dimensión ética de las inhibiciones injustificadas de los jueces es una cuestión de relevancia particular para la mayoría de los poderes judiciales de la región iberoamericana por los efectos negativos que pudiera tener en la tramitación y celeridad adecuada de los procesos. Cuando su ejercicio no encuentra sustento en las leyes, trasciende a la credibilidad de los sistemas de justicia y de los Estados democráticos que conforman el área, constituyéndose en un problema de alcance social. Y también desde el punto de vista del juez un abuso de las abstenciones puede encubrir actitudes dilatorias, puede reflejar problemas vinculados a la objeción de conciencia y puede crear un clima laboral inapropiado entre los colegas que ven aumentada su carga judicial.

7. En la XVIII reunión de la Comisión Iberoamericana de Ética Judicial, celebrada en Santo Domingo, República Dominicana, los días 20 y 21 de febrero de 2023, se acordó la realización de un dictamen relativo a las exigencias éticas frente a un exceso en la invocación de inhabilidades para juzgar, con fundamento en la tendencia a esta práctica observada en algunos sistemas judiciales en Iberoamérica.

II. La regulación de la inhibición en el ámbito iberoamericano

8. La inhibición del juez es una institución procesal vinculada a un derecho que también es garantía fundamental de salvaguarda de la imparcialidad, pero en su ejercicio se debe cuidar no dañar la confianza y credibilidad en la administración de justicia. El catálogo de motivos de la recusación incluye los que imponen la obligación de la inhibición, se trata de la enunciación de causas objetivas de inhibición, expresión de la responsabilidad de los jueces, lo cual implica una doble dimensión, de un lado, sustentada en la norma y, de otro, en el imperativo de la ética.

9. En la mayoría de los ordenamientos jurídicos de Iberoamérica existe coincidencia en las causas de recusación e inhibición que regulan sus disposiciones normativas. En el caso de la inhibición, estas similitudes en la identificación de las causas objetivas relacionadas a continuación, en modo alguno deben considerarse como limitativas, sino que más bien, como se puede comprobar a la vista de la legislación procesal dominicana, se trata de causas enunciativas:

1) Ser cónyuge, conviviente o pariente dentro del cuarto grado de consanguinidad o por adopción, o segundo de afinidad, de alguna de las partes o de su representante legal o convencional;

2) Ser acreedor, deudor o garante, el juez o la juez, su cónyuge o conviviente de alguna de las partes, salvo cuando lo sea de las entidades del sector público, de las instituciones bancarias, financieras o aseguradoras. En todo caso la inhibición o la recusación sólo son procedentes cuando el crédito o garantía conste en un documento público o privado reconocido o con fecha cierta anterior al inicio del procedimiento de que se trate;

3) Tener personalmente, su cónyuge o conviviente, o sus parientes dentro de los grados expresados en el ordinal 1), procedimiento pendiente con alguna de las partes o haberlo tenido dentro de los dos años precedentes si el procedimiento ha sido civil y dentro de los cinco años si ha sido penal. No constituyen motivo de inhibición ni recusación la demanda o querella que no sean anteriores al procedimiento penal que se conoce.

4) Tener o conservar interés personal en la causa por tratarse de sus negocios o de las personas mencionadas en el ordinal 1);

5) Ser contratante, donatario, empleador, o socio de alguna de las partes;

6) Haber intervenido con anterioridad, a cualquier título, o en otra función o calidad o en otra instancia en relación a la misma causa;

7) Haber emitido opinión o consejo sobre el procedimiento particular de que se trata y que conste por escrito o por cualquier medio lícito de registro;

8) Tener amistad que se manifieste por gran familiaridad o frecuencia de trato con cualesquiera de las partes e intervinientes;

9) Tener enemistad, odio o resentimiento que resulte de hechos conocidos con cualquiera de las partes e intervinientes;

10) Cualquier otra causa, fundada en motivos graves, que afecten a su imparcialidad o independencia.discriminatorio en las resoluciones judiciales.

III. La inhibición del juez como garantía del respeto a la imparcialidad

10. El derecho de inhibición del juez tiene una conexión importante con la imparcialidad. Es pertinente destacar que, en el orden etimológico, la palabra imparcialidad, conforme a la definición del *Diccionario de la Lengua Española* de la Real Academia, significa «Falta de designio anticipado o de prevención en favor o en contra de alguien o algo, que permite juzgar o proceder con rectitud». Por su parte, el vocablo imparcial está vinculado a la profesión de juez, por lo que podría decirse que el primer deber de un magistrado es la imparcialidad.

11. En el preámbulo de los *Principios de Bangalore sobre Conducta Judicia*l se proclama que la confianza pública en el sistema judicial, en la autoridad moral y la integridad del poder judicial es de extrema importancia en una sociedad democrática moderna; y con ese fin establece la obligación de los jueces de respetar y honrar las funciones jurisdiccionales como una encomienda pública, debiendo colaborar, mantener e incrementar la confianza en el sistema.

12. Los *Principios de Bangalore sobre Conducta Judicia*l vinculan la imparcialidad con la facultad de inhibición y se expresan así: «La imparcialidad es esencial para el desempeño correcto de las funciones jurisdiccionales. La imparcialidad se refiere no sólo a la decisión en sí misma, sino también al proceso mediante el cual se toma esa decisión». Además, agrega el Código de Ética de los Jueces

adoptado en el marco de las Naciones Unidas: «El juez no puede tener ningún interés en el asunto del que está apoderado y en términos generales deberá desempeñar sus tareas judiciales sin favoritismo, predisposición o prejuicio». Tal como se explica en el Comentario relativo a los Principios de Bangalore sobre Conducta Judicial debe recordarse la famosa sentencia del juez Hewart, de 1924, conforme a la cual: "Imparcialidad es ausencia de prejuicio y las apariencias en este ámbito son tan importantes como la realidad, porque de ellas dependen la percepción y la opinión de la sociedad sobre el tribunal con relación al caso"[1].

13. Con relación a la imparcialidad y su vinculación con la inhibición, ha de tenerse en cuenta la postura de la Corte Interamericana de Derechos Humanos conforme a la cual: «(…) la imparcialidad exige que el juez que interviene en una contienda particular se aproxime a los hechos de la causa careciendo, de manera subjetiva, de todo prejuicio y, asimismo, ofreciendo garantías suficientes de índole objetiva que permitan desterrar toda duda que el justiciable o la comunidad puedan albergar respecto de la ausencia de imparcialidad[2].

14. En esa misma línea, se dice que imparcial es el juez que resuelve conforme a derecho, libre de influencias ajenas y no tiene otros motivos para decidir que no sean los que le proporcionan la Constitución y la ley. Se dice del juez que es ajeno a cualquier relación, preferencia o sesgo que pueda afectar, o parecer afectar, a su capacidad para pronunciarse con total independencia[3]. Y por ello resulta de especial importancia la jurisprudencia del Tribunal Europeo de Derechos Humanos y del Tribunal de Justicia de la Unión Europea.

15. El Tribunal Europeo de Derechos Humanos, al interpretar el artículo 6 del Convenio -que protege el derecho a un juicio justo- sustenta que el juez no sólo debe ser imparcial, sino que también tiene que aparentar serlo. Dicho tribunal cita en su sentencia el adagio inglés «*justice must not only be done: it must also be seen to be done*» (No sólo debe impartirse justicia; también ha de verse cómo se imparte)[4].

---

1 *Comentario relativo a los Principios de Bangalores sobre Conducta Judicial*, Oficina de las Naciones Unidas contra la Droga y el Delito, Viena y Nueva York, 2013, apartado 56.

2 Corte IDH. Caso Apitz Barbera y otros ("Corte Primera de lo Contencioso Administrativo") Vs. Venezuela. Excepción Preliminar, Fondo, Reparaciones y Costas. Sentencia de 5 de agosto de 2008. Serie C No. 182.

3 Consejo Consultivo de Jueces Europeos, Informe nº 1 (2001) sobre las normas relativas a la independencia y a la inamovilidad de los jueces, Consejo de Europa, Estrasburgo, apartado 12.

4 Tribunal Europeo de Derechos Humanos, sentencia de 17 de enero de 1970, D*elcourt c. Bélgica,* CE:ECHR:1970:0117JUD000268965, apartado 31.

16. En el mismo sentido, este mismo Tribunal de Estrasburgo ha reiterado: «por lo general la imparcialidad se define como la ausencia de prejuicio o de inclinación y puede apreciarse de distintas maneras [...] de conformidad con una perspectiva subjetiva, que tiene en cuenta la convicción personal y el comportamiento del juez, es decir, se indaga si este ha demostrado que ha tomado partido o ha incurrido en un prejuicio personal en el caso concreto [...] o desde una perspectiva objetiva que consiste en determinar si el tribunal ofrece, especialmente a través de su composición, garantías suficientes para excluir cualquier duda legítima en cuanto a su imparcialidad»[5]; y en este último aspecto sustenta el Tribunal Europeo de Derechos Humanos: «todo juez en relación con el cual pueda haber razones legítimas para dudar de su imparcialidad debe abstenerse de conocer el caso ya que lo que está en juego es la confianza que los tribunales deben inspirar a los ciudadanos en una sociedad democrática»[6].

17. Por otra parte, el Tribunal de Justicia de la Unión Europea ha proclamado con el mismo espíritu: «las garantías de independencia e imparcialidad exigidas por el Derecho de la Unión postulan la existencia de normas que permitan excluir toda duda legítima en el ánimo de los justiciables en lo que respecta a la impermeabilidad de dicho órgano frente a elementos externos y en lo que respecta a la neutralidad de este ante los intereses en litigio»[7].

18. En la República Dominicana, el Tribunal Constitucional sostiene: «(…) para la justicia constitucional, el derecho a la exigencia de la imparcialidad del juez es considerado como parte esencial del debido proceso en el cual se reconozca dicha garantía fundamental para la aplicación de una correcta administración de justicia en un Estado de derecho (…)»[8].

---

5 Tribunal Europeo de Derechos Humanos (Gran Sala), sentencia de 6 de noviembre de 2018, *Ramos Nunes de Carvalho e Sá c. Portugal*, CE:ECHR:2018:1106JUD005539113 apartado 146.

6 Tribunal Europeo de Derechos Humanos (Gran Sala), sentencia de 15 de octubre de 2009, *Micallef c. Malta,* CE:ECHR:2009:1015JUD001705606, apartado 98.

7 Tribunal de Justicia de la Unión Europea, sentencia de 11 de mayo de 2023, *Inspecţia Judiciar*ă, C-817/21, EU:C:2023:391, apartado 47.

8 República Dominicana, Sentencia TC/0483/15, acápite 11.10, del seis (6) de noviembre del año dos mil quince (2015).

19. En España, bajo la influencia directa de los Tribunales europeos, el Tribunal Constitucional considera la imparcialidad judicial como garantía esencial de la función jurisdiccional y se expresa en dos sentidos, por un lado como noción subjetiva y por otro como noción objetiva, siendo la primera la que exige considerar cuanto sea ajeno a la administración del litigio y la segunda, la necesidad de que al decidir se asegure evitar un eventual contacto precedente con el caso[9]. Como garantía esencial del debido proceso, el derecho a la imparcialidad exige que la pretensión se resuelva por un tercero ajeno a las partes y a los intereses propios del litigio, que se someta exclusivamente al ordenamiento jurídico como criterio de decisión. Esto genera una obligación para quien juzga de apartarse o abstenerse de conocer en el caso de que concurran circunstancias que puedan hacer pensar a las partes y a la sociedad que es parcial. Así lo resume el Tribunal Constitución español: «Esta obligación de ser ajeno al litigio puede resumirse en dos reglas: primera, que el Juez no puede asumir procesalmente funciones de parte; segunda, que no puede realizar actos ni mantene conexiones de hecho que puedan poner de manifiesto o exteriorizar una previa toma de posición anímica a su favor o en su contra»[10] lograrlo, se requiere de una voluntad institucional.

VI. La dimensión ética del derecho a inhibirse desde la óptica del Código Iberoamericano de Ética Judicial

20. Los artículos 10 a 16 del Código Iberoamericano de Ética Judicial abordan y desarrollan la imparcialidad como principio ético. Por una parte, el artículo 10 contiene la descripción siguiente: «El juez imparcial es aquel que persigue con objetividad y con fundamento en la prueba la verdad de los hechos, manteniendo a lo largo de todo el proceso una equivalente distancia con las partes y con sus abogados, y evita todo tipo de comportamiento que pueda reflejar favoritismo, predisposición o prejuicio». Y a continuación el artículo 11 enuncia un deber ético de abstención en estos términos: «El juez está obligado a abstenerse de intervenir en aquellas causas en las que se vea comprometida su imparcialidad o en las que un observador razonable pueda entender que hay motivo para pensar así».

9 España. Tribunal Constitucional, sentencia nº 27/1981, de 20 de julio de 1981; y sentencia nº 11/2000, de 17 de enero de 2000.

10 España. Tribunal Constitucional, sentencia nº 140/2004, de 13 de septiembre, ponente: Pérez Vera, FJ 4.

21. Estas disposiciones definen el contexto ético que reviste esta institución; de su interpretación se deriva que se trata de una garantía que impone varias obligaciones éticas.

22. Por una parte, la función judicial impone la observancia de valores y principios condicionados y emanados del propio ordenamiento jurídico y de la sociedad, basados en la costumbre, la cultura y la moral pública y en los estándares éticos asimilados por las instituciones judiciales, por lo que el abuso de la inhibición por quienes imparten justicia requiere particular atención, más allá del plano normativo formal por tratarse de una cuestión que gravita en el plano de la ética.

23. Por otra parte, la gestión razonable del uso de la inhibición impone a los diferentes sistemas judiciales velar por una conducta que se corresponda con la visión de administrar justicia en tiempos difíciles donde prevalece la exposición de los jueces al escrutinio público, que, por tanto, deben actuar en todos los actos de la vida privada convencidos de su trascendencia pública, por lo que resulta necesaria la protección no solo de quien se abstenga de conocer un proceso sino de la institución a la que pertenece, de cara a la salvaguarda de la integridad de la función jurisdiccional.

24. Es reprochable, desde el punto de vista ético, la presentación de una solicitud por la parte que persiga la recusación cuando la persona que juzga ya tuviese conocimiento de las causas que la sustentan porque si no declara su abstención no solo vulnera el Código Iberoamericano de Ética Judicial sino que también transgrede el ordenamiento constitucional y convencional y conculca los derechos fundamentales del justiciable.

25. El abuso en la formulación de la recusación, fundada en artificios jurídicos, es expresión de la temeridad y la deslealtad procesal y no debieran fabricarse causas que persigan provocar la inhibición forzada lo que amerita poner atención a ese panorama de la administración de justicia que genera trastornos considerables al proceso.

26. En algunos de los sistemas de administración de justicia de la región iberoamericana se ejerce frecuentemente el derecho de inhibición, con una tendencia colectiva, respecto a la que se debe estar en alerta porque, si bien es cierto que la abstención protege la garantía de la imparcialidad

como derecho fundamental, no lo es menos que su ejercicio impone una evaluación de las causas, con apego a las convicciones y valores de la judicatura, sobre todo cuando se sustente en cuestiones subjetivas, que no están tasadas expresamente en la legislación correspondiente.

27. La importancia de la imparcialidad judicial radica en la necesidad de su existencia como garantía del debido proceso, se trata de un ámbito propio de la legitimación de la administración del proceso y de la función judicial como parte ajena a los intereses del litigio. A la judicatura le corresponde, en los casos de inhibición, la solución de un conflicto intersubjetivo de intereses sobre la base del respeto a los derechos que sean objeto de tutela judicial efectiva y teniendo en cuenta la dimensión ética que supone.

VI. Conclusiones

28. La institución de la inhibición supone la abstención de conocer un proceso determinado, constituye un acto de responsabilidad en el contexto de la función judicial y se erige en salvaguarda de un derecho fundamental para proteger la integridad del sistema de administración de justicia.

29. La inhibición encuentra su fundamento en causas y presupuestos debidamente tasados por el orden normativo, objetivos o subjetivos, pero, en cualquier caso, en las personas que imparten justicia debe prevalecer un comportamiento ético intachable, representativo de la integridad y la probidad que se espera de su ejercicio, ya sea que la abstención se presente de forma individual o colectiva.

30. El abuso del derecho a la inhibición puede afectar el curso adecuado de la administración de justicia cuando atenta contra el principio de celeridad procesal, cuestión que los integrantes de la judicatura deben sopesar, particularmente cuando se aleguen causas que no se correspondan con las reguladas por el ordenamiento de cada país.

31. El uso del derecho a la inhibición es un pilar que potencia la transparencia de la actuación de los sistemas de justicia, pero su ejercicio no debe desbordar los límites impuestos no solo por su configuración procesal sino por la dimensión ética en la que se desarrolla la función jurisdiccional, sustentada en los valores y principios recogidos por el ordenamiento jurídico de cada sociedad.

VII. Recomendaciones

32. Los sistemas de impartición de justicia de los países de Iberoamérica deben adoptar medidas de salvaguarda, claras y precisas, con relación al abuso del derecho de inhibición por los integrantes de la judicatura, que incluyan el enfoque ético del problema, cuando atenta contra la efectividad de la administración de justicia, la legitimidad de los sistemas judiciales y la confianza de los ciudadanos en el Estado de derecho.

33. Los magistrados que formulen su inhibición deben asumir que tal pretensión implica una dispensa o excepción al normal desempeño, objeto de un inicial y genuino juramento ético y legal. Por ello debe estar impregnado de honradez intelectual, probidad, lealtad y buena fe, y su correlato en los subrogantes que juzgan su admisibilidad, máxime si no existe posibilidad de revisión, ante la decisión adversa.

34. No parece la mejor garantía ética que los magistrados receptores de una causa o expediente en virtud de una eventual inhibición, sean los que examinen y juzguen su procedencia.

35. Se considera susceptible de reproche ético, la utilización indebida e inescrupulosa del pedido de apartamiento o inhibición, y violatoria de la garantía del debido proceso legal.

36. La responsabilidad institucional en la judicatura, exige transparencia, seriedad y celeridad para establecer el juez natural cuando existan planteos de inhibición o recusación, priorizando la confianza y credibilidad en la Administración de Justicia.

37. Como se deduce del art. 10 del Código en su parte pertinente, «El juez imparcial es aquel….evita todo tipo de comportamiento que pueda reflejar favoritismo, predisposición o prejuicio». No obstante y de producirse esta situación, por razones de profunda convicción moral que produzca un grave y notorio impedimento al principio de imparcialidad, podrá excepcionalmente ser analizada y ponderada esa objeción de conciencia, en orden a los principios y valores en juego.

PROYECCIÓN PÚBLICA DE LA VIDA PRIVADA DE LOS JUECES Y SU RELEVANCIA ÉTICA

PONENTE: COMISIONADA FARAH M. SAUCEDO PÉREZ

VIGESIMOSEXTO DICTAMEN, DE 8 DE SEPTIEMBRE DE 2023, DE LA COMISIÓN IBEROAMERICANA DE ÉTICA JUDICIAL

I. Introducción

1. La Comisión Iberoamericana de Ética Judicial[1] dedica una parte importante de su labor a incentivar, en los integrantes de los sistemas judiciales de la región, una conducta acorde con los principios y virtudes consagrados en el Código Iberoamericano de Ética Judicial, en correspondencia con los Objetivos de Desarrollo Sostenible aprobados por la Organización de las Naciones Unidas, ONU, en 2015 y de la Agenda 2030 para el Desarrollo Sostenible, instrumentos internacionales que inspiran también la actuación de la Cumbre Judicial Iberoamericana.

2. En la reunión celebrada el 21 de febrero de 2023 en la ciudad de Santo Domingo, capital de República Dominicana, la Comisión Iberoamericana de Ética Judicial acordó, con el voto unánime de sus miembros, elaborar un dictamen en el que se abordara el tema referido a la proyección pública de la vida privada de los jueces y su relevancia ética.

3. La idea de este dictamen tiene antecedentes en varios de los pronunciamientos realizados por la Comisión Iberoamericana de Ética Judicial[2] la que al tratar algunos de los dilemas éticos afrontados por los integrantes de la judicatura, no ha soslayado su relación con la vida privada de estos, en el entendido de que el comportamiento de los jueces, ya sea en el ámbito público o privado, es una cuestión de interés para los estados miembros de esta área geográfica y cultural; por esa razón, este dictamen propone un enfoque actual del asunto, con la intención de motivar la reflexión y el debate en torno a un conflicto ético de origen antiquísimo que no ha perdido su vigencia en la sociedad moderna.

---

1 «(…) de no haberse creado una institución encargada de interpretar y desarrollar estos principios y virtudes, nada se hubiese conseguido en la práctica (…)».*Comentarios a los dictámenes de la Comisión Iberoamericana de Ética Judicial.* Escuela Nacional de la Judicatura, Santo Domingo, 2023, pp. 19.

2 «Las juezas y los jueces deben conocer cómo las acciones que realizan en los ámbitos de su vida privada pueden tener trascendencia pública y afectarles laboralmente, así como a la imagen de la institución y la administración de justicia en general». Ver en Dictamen décimo sobre *La formación en principios y virtudes judiciales en ob.cit*., pp. 293.

II. Acerca de la conducta de los jueces

4. En la tradición cultural occidental la *Biblia* narra que un día Moisés se dedicó a la tarea de juzgar, mientras era observado por su suegro que, impresionado por el rigor de la faena, le recomendó: «(…) escogerás de entre todo el pueblo hombres capaces, temerosos de Dios, hombres veraces que aborrezcan la avaricia (…)»[3], y así fue como surgieron del pueblo personas capaces de juzgar. En el libro *Jueces* se cuentan historias como la de Débora, que fue la única mujer entre ellos y la más virtuosa; al contrario de otros que, como Sansón, no lo fueron tanto, poniéndose de manifiesto la humanidad del modelo bíblico de juez.

5. A partir del siglo XVI y durante el período colonial los Reyes de Aragón y Castilla decidieron compartir esta función con otras personas que juzgaban en su nombre, entre ellas, los oidores, a quienes se les exigió en las provincias americanas «(…) dotes de ciencia, prudencia y demás virtudes que continuamente se requieren en los demás magistrados sino que aun sean los más aventajados en ellas que ser pudiere, y por consiguiente se elijan de los mejores, más probados y experimentados sujetos (…)»[4].

6. La monarquía portuguesa, del mismo modo que la española, utilizó varios cargos para la administración de justicia en las colonias americanas, entre ellos el de los jueces de fuero, oidores generales y desembargadores, de quienes se esperaba un buen comportamiento, que era verificado al término de su mandato, dándose a los súbditos la oportunidad de hacer denuncias por los desvíos, en los llamados juicios de residencia, donde resultaba común interrogar a los testigos en cuanto a si los funcionarios habían dormido con algunas mujeres llevadas ante ellos, indagación que evidentemente atañe a su conducta personal.

---

3 *Éxodo 18.21*. Ver en *Biblia* https://www.bible.com

4 De Solórzano Pereira, J. *Política Indiana.* https//www.erlibro.com., p. 776.

7. Estos antecedentes demuestran la preocupación de las diferentes sociedades, incluidas las del espacio geopolítico iberoamericano, por el comportamiento de las personas que se dedicaban a impartir justicia, puntales de la credibilidad del poder en cuyo nombre actuaban.

8. En las postrimerías del siglo pasado, la ONU, formuló las reglas de conducta para los jueces, conocidas como *Principios básicos relativos a la independencia de la judicatura*, que entre otros aspectos regula, en su artículo 8, que «(…) los jueces deben comportarse en todo momento de forma tal que queden aseguradas la dignidad de su cargo y la imparcialidad e independencia de su jurisdicción»[5], en alusión a la repercusión de la conducta privada de los jueces en su ámbito profesional.

9. A la iniciativa anterior le siguieron, en 2002, los conocidos internacionalmente como *Principios de Bangalore sobre la Conducta Judicial*, en cuyo preámbulo se enuncia: «Una judicatura de integridad inobjetable es la institución básica fundamental que garantiza la vigencia de la democracia y la legalidad. Incluso cuando faltan todas las protecciones, una judicatura de esas características ofrece al público un baluarte contra los atropellos a los derechos y libertades garantizados por la ley»[6].

10. A este código le sucedieron otros pronunciamientos regionales sobre la cuestión, hasta llegar al *Código Modelo Iberoamericano de Ética Judicial* (2006), adoptado por la Cumbre Judicial Iberoamericana, lo que apunta a la vigencia de un debate que, al día de hoy, no concluye y que se extenderá en el tiempo por su profundo calado humano e importancia para la sociedad.

---

5 Principios básicos relativos a la independencia de la judicatura. Ver en https://www.chchr.org

6 Weeramantry, C.G., *Prefacio al Comentario relativo a los principios de Bangalore sobre la Conducta judicial*. Oficina de las Naciones Unidad contra la Droga y el Delito. Viena, 2019, pp.1

II. La vida privada de los jueces y las exigencias de la ética judicial

11. La profesión de juez comúnmente se asocia con la virtud; se dice que un juez es virtuoso cuando es versado en leyes y en la vida práctica, además de honesto y justo. Esta noción sobre el ideal de juez, nacida en la antigüedad, llega hasta la contemporaneidad como un axioma: es una profesión que demanda estándares elevados de conducta a quienes la ejercen, necesarios para resolver con acierto los asuntos sometidos a su conocimiento. A tono con esta visión, el Código Iberoamericano de Ética Judicial declara: «(…) El poder que se confiere a cada juez trae consigo determinadas exigencias que serían inapropiadas para el ciudadano común que ejerce poderes privados; la aceptación de la función judicial lleva consigo beneficios y ventajas, pero también cargas y desventajas(…)»[7], las que son asumidas conscientemente por los jueces, en tanto el ejercicio mismo de la profesión contribuye a su asimilación, fruto de un proceso de mejoramiento profesional y humano continuo.

12. Los jueces, en su tránsito por la judicatura, deben afianzar esas virtudes, en la medida que a ese objetivo tributan los procesos de formación implementados por los diferentes sistemas judiciales, los postulados de los códigos de ética judicial, las regulaciones de las leyes orgánicas, las normas de los textos constitucionales y el ejemplo de otros jueces atesorado en la memoria de cada fuero judicial; sin embargo, en no pocas ocasiones, su actuación en la vida privada deviene fuente de cuestionamientos, incluso más enérgicos que los generados por el incumplimiento de reglas relacionadas con la función judicial. Expuesto así, pudiera parecer que los límites entre la vida profesional y la vida privada de los jueces están muy bien definidos y que solo se trata de estar atentos para que no se produzcan contaminaciones entre una y otra; pero el problema es mucho más difícil.

13. La complejidad del concepto de vida privada, su evolución constante en la modernidad y la mutación de sus contenidos, avalan la conveniencia, a los fines de este dictamen, de asumir, como premisas para su manejo, que la conducta del juez se aviene a cánones éticos extensivos a las diferentes esferas de su comportamiento en los distintos ámbitos donde se desenvuelve

7 *Código Iberoamericano de Ética Judicial.* Ver en https://www.poderjudicial.es, pp. 3.

y que el contexto donde se aplican se transforma continuamente, tal como acontece con la sociedad en su conjunto. A estas exigencias, se añade la de ofrecer un servicio judicial de calidad y, dicho así, ha llevado a algunos a pensar que se trata de una profesión semejante a un "sacerdocio", que segrega a los jueces a una suerte de gueto profesional donde permanecen, a salvo de las "tentaciones" del entramado social y, a la vez, los preserva para impartir la justicia que de ellos se espera.

14. Ahora bien, cada juez enfrenta con sus herramientas personales los desafíos de su tránsito por la carrera judicial; sin embargo, las instituciones judiciales no actuarían con la responsabilidad debida, si consintieran que sus integrantes se enajenen, de modo consciente o inconsciente, de la sociedad en la que viven, porque el conocimiento de las realidades de las que estos profesionales forman parte se obtiene, en gran medida, como resultado de su experiencia vital; un buen juez no se coloca a la vera de la sociedad, sino que participa en ella, como se espera que haga un buen juez.

IV. Vida privada de los jueces y su proyección pública

15. El interés por identificar algunos comportamientos judiciales impropios conduce a la definición que los asocia con «(…) aquellos que en términos generales afectan o parecen afectar las prácticas virtuosas de los jueces, en cuanto tal conducta se produce mientras el juez está ejercitando biográficamente un cumplimiento activo del rol social que la judicatura le impone. Esto es: en todas aquellas circunstancias temporales o materiales en las cuales sólo se explica su participación por el mismo ejercicio del rol público institucional que tiene. Abarca tanto las conductas que tienen lugar en el ejercicio de la función judicial como aquellas que se realizan fuera de ella pero que tienen una determinada trascendencia»[8]. Esta definición se corresponde con la visión del Código Iberoamericano de Ética Judicial, que mantiene su vigencia en la medida que retrata situaciones que en la actualidad siguen teniendo lugar entre los integrantes de los sistemas judiciales.

8 Ídem Andruet (h), A. *"Ámbito de los comportamientos judiciales impropios (I). Comercio y Justicia*, publicado el 19-10-16. Ver en https://comercioyjusticia

16. En ocasiones, los jueces o uno de los miembros de su familia estrechan vínculos de amistad o de otro tipo con terceros, los que si bien tienen lugar fuera de la sede judicial, en el ámbito privado de sus relaciones personales, generan la desconfianza con respecto a su actuación, dado que esas relaciones pudieran influir en las decisiones judiciales que adopten o dar a entenderlo; para evitar esta situación, no es necesario que los jueces renuncien definitivamente a esos vínculos, (deben hacerlo mientras estén a cargo del proceso que los involucra, excusándose de la obligación de su conocimiento con amparo en las normas procesales), para no apartarse del cumplimiento de su deber de imparcialidad.

17. La utilización por los jueces de las facultades que les confieren las leyes para el ejercicio de la función judicial, en beneficio personal, de su familia o de cualquier persona conocida, con el objetivo de resolver alguna cuestión relacionada con las atribuciones de otras instituciones, no les está permitido; por el contrario, han de abstenerse de hacer uso de su influencia, si están dispuestos a actuar con la corrección que se espera de ellos; del mismo modo, no deben utilizar los recursos materiales puestos a su disposición para ejercer sus funciones, al servicio de sus intereses personales, porque estas conductas los apartan del modelo de juez virtuoso, apegado al decoro requerido por esta profesión, una virtud que los compulsa también a la decencia de su vestuario y modales, más allá de las puertas de la oficina judicial, tanto en los espacios físicos como virtuales, donde no siempre respetan las reglas impuestas por la sociedad.

18. La interacción de los jueces en las redes sociales se encuentra entre los aspectos más debatidos en la actualidad en materia de ética judicial y si esa interacción se relaciona con cuestiones vinculadas a su vida privada, la polémica, en no pocos casos, se ha extendido globalmente, lo que es posible dada la utilización cada vez más creciente de las nuevas tecnologías, un fenómeno de aparición relativamente reciente y de efectos múltiples en la vida de las personas.

19. En los diferentes países que conforman la región iberoamericana, el comportamiento de los jueces en las redes sociales no es homogéneo: un reducido grupo opta por mantenerse alejado de las plataformas digitales, para evitar los riesgos que supone el tráfico de la información y el almacenamiento de datos personales; mientras que la mayoría las utiliza en función de su actividad profesional y para cuestiones de las llamadas “personales”, o sea, de su vida privada.

20. En las redes sociales las publicaciones de contenidos relacionados con los vínculos interpersonales, familiares, viajes, festejos, aficiones, entre otros aspectos de la vida privada de los jueces, convierten a tales plataformas en una pasarela virtual de su vida privada y provocan una sobreexposición de la imagen de estos en los medios digitales. La realización de estas publicaciones personales fuera del ámbito judicial y como consecuencia del ejercicio del derecho a la libre expresión son algunos de los argumentos utilizados por quienes niegan la repercusión de estas en la credibilidad de la función judicial, manifestaciones que validan lo ya dictaminado por la Comisión Iberoamericana de Ética Judicial en cuanto a que:«(…) Aun cuando las personas juzgadoras merecen y se les reconoce el derecho a su intimidad, deben saber que cualquier acto u opinión que sea conocido de forma pública, podrá ser vinculado con su competencia profesional, por lo que sus relaciones personales, familiares y sociales deben estar también orientadas bajo el marco de los principios éticos judiciales»[9].

21. Los procesos de globalización y de informatización de la sociedad moderna conducen a que cada día resulte menos posible mantener a salvo de la publicidad las cuestiones relacionadas con la vida privada de los jueces, ya sea porque forman parte de los datos personales que las plataformas digitales se encargan de almacenar, aun si no fueran "publicados", o porque el uso de estas tecnologías inevitablemente ha pautado las relaciones de todas las personas con acceso a ellas, aunque no siempre lo reconozcan, de suerte que los espacios privados, cada vez son menos y es casi una verdadera utopía pretender preservarlos, una disyuntiva que no solo enfrentan los jueces, sino todas las personas, en sentido general.

22. La repercusión de la vida privada en la función pública de los jueces, no obstante, la indeterminación entre una y otra por las razones apuntadas, es una cuestión que se debe atender, sin descuidar, al menos, tres elementos fundamentales: la protección de los derechos individuales de los jueces, la ponderación adecuada del impacto de ese acto de su vida privada en la función pública que realizan y la gravedad de la ofensa, en atención a la percepción que la comunidad tiene de la conducta de los jueces, la que depende de los patrones mayoritariamente asumidos por la sociedad, los que pueden variar de acuerdo con el lugar y el tiempo.

9 Montero Montero, J y Andruet (s) A. *Dictamen décimo de la Comisión de Ética Judicial ver en Comentarios a los dictámenes de la Comisión Iberoamericana de Ética Judicial*. Escuela Nacional de la Judicatura, Santo Domingo, 2023, pp. 293.

23. Los jueces ocupan un lugar activo en la materialización del Estado de Derecho en tanto el principio de integridad judicial les exige que sean los mejores guardianes del respeto a la Constitución, las demás leyes y los derechos fundamentales de las personas, erigiéndose así en garantes de la democracia; por estas razones, su conducta no puede ser menos que irreprochable[10] de acuerdo con las reglas de comportamiento permitidas por la sociedad.

V. Conclusiones

24. La repercusión de la vida privada de los jueces en sus funciones públicas es una cuestión a la que los sistemas judiciales de la región iberoamericana deben prestar atención permanente porque la violación de los principios éticos en el ámbito privado también pone en riesgo la credibilidad de la función judicial que desempeñan y resienten la confianza de la ciudadanía en la administración de justicia.

25. La proyección pública de la vida privada de los jueces se acrecienta en la modernidad, bajo el influjo de la globalización y la expansión constante de las tecnologías de la información y la comunicación social; por eso, la participación de los jueces en las redes sociales recaba que estos sean conscientes de las implicaciones de sus interacciones en el espacio digital, particularmente las que estén relacionadas con su vida privada; y de la influencia que estas pueden tener en la imagen de integridad de la judicatura.

26. La relevancia ética de la proyección pública de la vida privada de los jueces es fuente de polémicas en la contemporaneidad, relacionadas con la determinación de los comportamientos judiciales impropios, el respeto de los derechos fundamentales y su ejercicio responsable o la identificación de las personas idóneas para evaluar la actuación del juez, entre otros aspectos que justifican la necesidad de colocar este debate en la agenda de las instituciones judiciales que apuestan por la integridad de los jueces y la calidad del servicio judicial.

---

10 *Comentario relativo a los principios de Bangalore sobre la Conducta judicial.* Oficina de las Naciones Unidad contra la Droga y el Delito. Viena, 2019, pp.77.

VI. Recomendaciones

27. A las instituciones judiciales de Iberoamérica la Comisión recomienda:

a. Continuar promoviendo la formación en valores y principios éticos de los integrantes de la judicatura, que incluye su perfeccionamiento y actualización, si se trata de fomentar y afianzar en los jueces una conducta ética que consolide la credibilidad de los ciudadanos en los sistemas de justicia y, con ella, la confianza en las instituciones judiciales.

b. Establecer en los sistemas judiciales mecanismos eficaces que permitan la identificación de los comportamientos inadecuados de los jueces en su vida privada que impacten en la función judicial que ejercen, y corregirlos, si fuera el caso, con la diligencia que demande la entidad de las transgresiones.

c. Insistir en que –tal como se ha propuesto en dictámenes anteriores– cuando se lleve a cabo una reforma del Código Iberoamericano de Ética Judicial, se incluya alguna referencia a la conducta de los jueces en las redes sociales, en relación con su vida privada y, en correspondencia con ella, se actualice su lenguaje en atención a la impronta que el desarrollo de las tecnologías de la información y la comunicación social ha marcado en todas las esferas de la sociedad, incluida la impartición de justicia.

EL INTERNET DE LAS COSAS, LA CIBERSEGURIDAD Y LA INTELIGENCIA ARTIFICIAL, USOS, BENEFICIOS Y RIESGOS.

¿ESTÁ COSTA RICA PREPARADA VERDADERAMENTE?

FIORELLA ROJAS BALLESTERO[1]

1 Criminóloga y Criminalista de la UNED, Máster en Intervención Delictiva y persecución penal de la Escuela Internacional en Criminología y Criminalística, España. Laboratorista Forense y Perito Judicial del Departamento de Ciencias Forenses, OIJ.

Resumen

El objetivo de este artículo es dar una visión desde las ciencias criminológicas y la criminalística sobre el uso de la inteligencia artificial tomando como base el Internet de las cosas *(Internet of Things*) IoT y la seguridad virtual cuando se emplea esta tecnología. Metodológicamente, se utilizó una encuesta para verificar el conocimiento de las personas usuarias sobre el IoT. Luego se hizo una revisión bibliográfica y de normativa para verificar si el marco legal vigente era suficiente al usar dispositivos tecnológicos sin temor. Así se arrojó el resultado de que las personas sentían cierto grado de desconfianza al usar el Internet; pero al mismo tiempo no se preocupaban cuando utilizaban el IoT, el cual se creó como una forma de aumentar la productividad, reducir costos de producción y, al mismo tiempo, estudiar en tiempo real el comportamiento de la persona usuaria con el producto adquirido. El IoT comenzó a generar datos, algunos de ellos sensibles, lo que permitió que la línea de la creación y uso de bases de datos fuera lo suficientemente delgada como para cruzarla y delinquir con los datos de las personas y las empresas, por lo que había muchos riesgos en su uso. Se recomienda, por tanto, robustecer la normativa en protección de datos y los protocolos de ciberseguridad como estrategia de ciberdefensa nacional, pues tanto las personas como el sector privado y el Estado son susceptibles al robo de datos por no tener buenas prácticas y protocolos sobre el uso del IoT.

Palabras clave: ciberseguridad, protección de datos, estrategia de defensa cibernética.

Introducción

¿Qué se entiende por el Internet de las cosas (IoT)? Primero se debe revisar un poco qué es la tecnología inalámbrica, qué son los dispositivos móviles inteligentes, pues se puede visualizar el IoT entonces como una fuente para recolectar datos que ha venido creciendo exponencialmente. De esta forma, todo objeto conectable es un potencial originador de datos, abriéndose así la posibilidad de hacer análisis estadístico y predictivo de los datos recopilados, tales como el *big data* (macrodatos) y el *cloud computing* (la computación en la nube).

La tecnología ha venido evolucionando a pasos agigantados, desde que, en 1888, Rudolf Hertz comenzó a transmitir sin cables usando ondas electromagnéticas, hasta 1971, cuando unos investigadores de la Universidad de Hawaii crearon la primera red de área local inalámbrica (WLAN). Después, en 1999, Nokia y *Symbol Technologies* crearon WECA (*Wireless Ethernet Compability Alliance*), la cual, en el año 2003, se le cambió el nombre por Wi-Fi (*Wireless Fidelity*).

Por tanto, el uso de dispositivos inalámbricos ha sido vertiginoso. Ejemplo de ello ha sido el teléfono que pasó de ser un elemento fijo en la pared a un dispositivo cada vez más pequeño y portátil, hasta el nacimiento del teléfono celular que, si bien empezó con un tamaño grande, el hecho de no depender a un cable facilitó que la gran mayoría de las personas pudieran acceder a la comunicación de forma más ágil desde el lugar que fuera, según la conectividad de la que se dispusiera.

Así algunas personas pueden estudiar o teletrabajar en la playa o en la montaña, aunque aún existe una brecha muy grande en cuanto a accesibilidad y disponibilidad tanto de dispositivos como de red, y la tecnología inalámbrica ha venido a dinamizar mucho la gran mayoría de las telecomunicaciones del orbe y sus usos derivados.

Al mismo tiempo que el teléfono evolucionaba y el Internet iba apareciendo, se vio la posibilidad de poder hacer conectividad de muchos aparatos y dirigirlos desde el teléfono gracias a esas conexiones.

Luego, gracias a la activa forma de vivir del ser humano, quien necesita tener la información y el control de casi todo, surge el teléfono inteligente donde se tiene prácticamente una computadora mejorada. Por este medio, no solo se hacen llamadas telefónicas, sino también se puede interactuar socialmente a través de mensajes de texto, mensajes por aplicaciones como Messenger, WhatsApp y otras, se puede expresar las ideas que surgen en ese momento como en Twitter, compartir la foto del momento como en Instagram, o bien, observar lo que otras personas cuentan sobre ellas en Facebook y, al mismo tiempo, opinar sobre sí mismo(a).

También se puede comprar desde un libro hasta el diario de la alacena desde el *smartphone*, se puede agendar una cita médica, una cita legal, concertar entrevistas, conocer personas de otros países, ya sea a través de conferencias virtuales, clases virtuales, hasta se puede obtener una carrera profesional a través de un teléfono, si se necesita despertar a una hora en específico, o bien, si urge recordar algo, se puede programar una alarma; si se necesita saber una dirección, se puede acceder a *maps*.

Incluso hay *smartphones* con brújulas y un sinfín de accesorios y aplicaciones. Puede afirmarse que el dispositivo casi ha desplazado a las *laptops, tablets, iPad* y similares, aunque estos últimos se siguen ofertando, pues por comodidad es más fácil hacer algunas actividades en ellos, como escribir un ensayo, trabajar en una hoja de cálculo o leer libros digitales, entre otras actividades.

Al usar los dispositivos móviles con los ejemplos que se acaban de mencionar, se va creando la huella digital (diferente y, por mucho, a la huella dactilar), pues se va dejando un historial cibernético de los movimientos que la persona suele realizar, el banco donde hace sus transacciones, la municipalidad donde paga sus impuestos, las *website* de su preferencia, las búsquedas de información que ha realizado, los lugares que ha frecuentado, cómo es la casa donde vive, el auto que maneja, los hijos y las hijas que tiene, los colegios donde estudian, y se comienza a ventilar mucho dato sensible, algunos públicos por voluntad propia y otros datos privados que podrían volverse públicos.

Surgen el almacenamiento de datos y el estudio de estos para su uso en el mercado. Según el comportamiento de las personas, se comenzaba a saber cuáles eran los gustos de las personas en relación con las marcas de sus productos favoritos, en qué lugar se compraban, el uso que le daban.

Nace entonces el mercado de objetos inteligentes: autos que se encienden con comando de voz; refrigeradoras que indican cuándo los productos se van venciendo y así envían los datos a los dispositivos inteligentes; monitores de salud (presión, latidos, gasto de

calorías, pasos dados) que pueden almacenar esos datos y enviarlos a bases de datos médicas, entre tantas otras aplicaciones que han surgido.

Se crea así una recolección de muchos datos personales que deben almacenarse en algún lugar y cuyo acceso y uso no son tan restringidos ni personales, por lo que la cotidianidad, gustos y otros datos sensibles son casi de dominio público, y eso debe regularse tanto en el ámbito social como legal y normativo, en especial cuando el uso biométrico y el personal de los datos podrían generar un uso indebido de ellos provocando delitos que no tienen un marco regulatorio que los pueda tipificar como tales.

Este artículo pretende crear cierta conciencia sobre el almacenamiento, acceso y uso que se den a los datos que cada persona genera, según los objetos o cosas inteligentes que posea, las bases de datos que se crean en las diferentes empresas que proveen servicios a través del Internet de las cosas (en adelante IoT), así como también lograr determinar una guía para la regulación normativa del uso y la protección de los datos; aunque en Costa Rica exista una agencia de protección de estos denominada Agencia de Protección de Datos de los Habitantes (Prodhab), de la cual muchas personas desconocen su existencia.

Así mismo, desde el punto de vista criminológico y criminalístico, se pretende aportar la prevención del riesgo y el análisis de la investigación de la ocurrencia del delito para ir reduciendo la impunidad en este tipo de delitos.

Metodología

Se realiza una investigación cualitativa iniciando con el Internet de las cosas, para ir descubriendo poco a poco que, junto con la inteligencia artificial y la ciberseguridad, si las personas e instituciones públicas y privadas no tienen altas competencias digitales, la seguridad de todos los datos que se van dejando con la huella digital al usar el Internet en los dispositivos móviles de cualquier sistema operativo puede convertirse en un factor de muy alta vulnerabilidad para ser víctima de estafas o, peor aún, de ciberataques por grupos cibercriminales organizados de alto perfil peligroso.

Con base en las cualidades del problema, el alto uso del Internet de las cosas y la poca educación en ciberseguridad, se va dando paso a las posibles soluciones y recomendaciones que se deben llevar a cabo para no tener el tema de la ciberseguridad como un tema más dentro del Plan Anual Operativo de cada empresa, sino como una política pública de defensa y seguridad nacional.

Para tratar de tener una idea sobre lo que las personas conocen sobre el Internet de las Cosas, se realizó una pequeña encuesta y se socializó por las redes sociales Facebook y WhatsApp. De esa forma, también se podía conocer la interacción de ciertos grupos etarios en las redes sociales.

La siguiente información se desprende de dicho instrumento :

1. Escolaridad

2. Grupos de edad

3. Zona de residencia

4. Provincia de residencia

5. Género

6. ¿Sabe usted lo que es el Internet de las cosas?

7. ¿Está preocupado por la seguridad de sus datos y su privacidad en Internet?

8. ¿Cree que el Internet de las cosas va a suponer un cambio positivo o negativo?

9. ¿Aceptaría y se sentiría seguro de que sus datos estén al alcance de todo el mundo?

10. ¿Aceptaría viajar en un automóvil autónomo (sin conductor)?

11. ¿Cree que el mundo está preparado para el IoT?

12. Deseo de aprender más sobre el tema.

Se trató de una encuesta pequeña diseñada tan solo para averiguar qué tanto se relaciona y conoce del tema. Se hizo usando un *smartphone* mediante un formulario electrónico creado en sistema operativo Android a través de la aplicación Google Forms y socializado en las redes sociales Facebook y WhatsApp; es decir, se usó el IoT para averiguar y escribir sobre el IoT.

La tabulación de los datos y la elaboración de los gráficos se realizaron en una hoja de Excel de Office 365 en una laptop con sistema operativo Android y con las diferentes fórmulas estadísticas que dicho *software* posee.

La población final fue n=33, de estas, 16 personas (48.5%) se percibieron de género masculino, y 17 personas (51.5%) de género femenino. (Figura 1).

13 personas eran de un rango de edad de menos de 18 años a 29 años cumplidos (39.4%); 17 personas en un rango de edad de 30 a 49 años (51.5%) y 3 personas de 50 a 79 años (9.1%) (Figura 2), evidenciándose que la mayor cantidad de personas que respondieron la encuesta se encontraban en una edad económicamente activa y habían visto el nacimiento del Internet y la evolución de los dispositivos de comunicación. En segundo lugar, se encontraba una población más joven, nacida luego de la creación del Internet y los sistemas operativos, pero había ido evolucionando y desarrollándose junta.

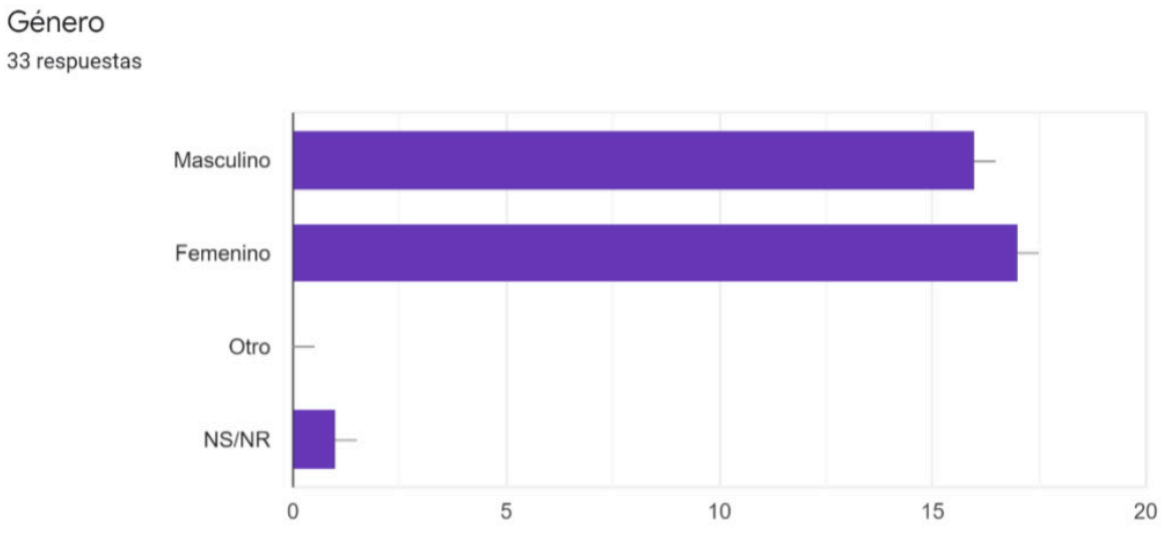

Figura 1. Género de las personas encuestadas. Fuente: elaboración propia.

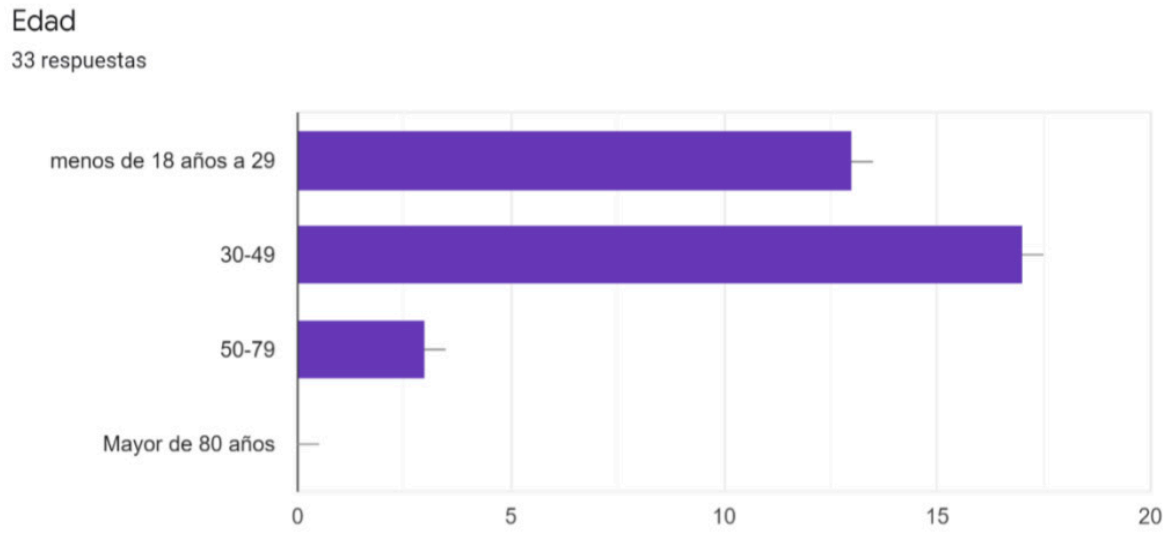

Figura 2. Rango de edad. Fuente: elaboración propia.

Con respecto a la escolaridad, un 15.2% (5 personas) tenía secundaria completa; un 21.2% (7 personas) tenía incompletos sus estudios universitarios; un 48.5% (16 personas) ya concluyó sus estudios universitarios y un 21.2% (7 personas) había obtenido al menos un postgrado (Figura 3). Este dato también es consistente con el rango de edad de las personas que respondieron el cuestionario.

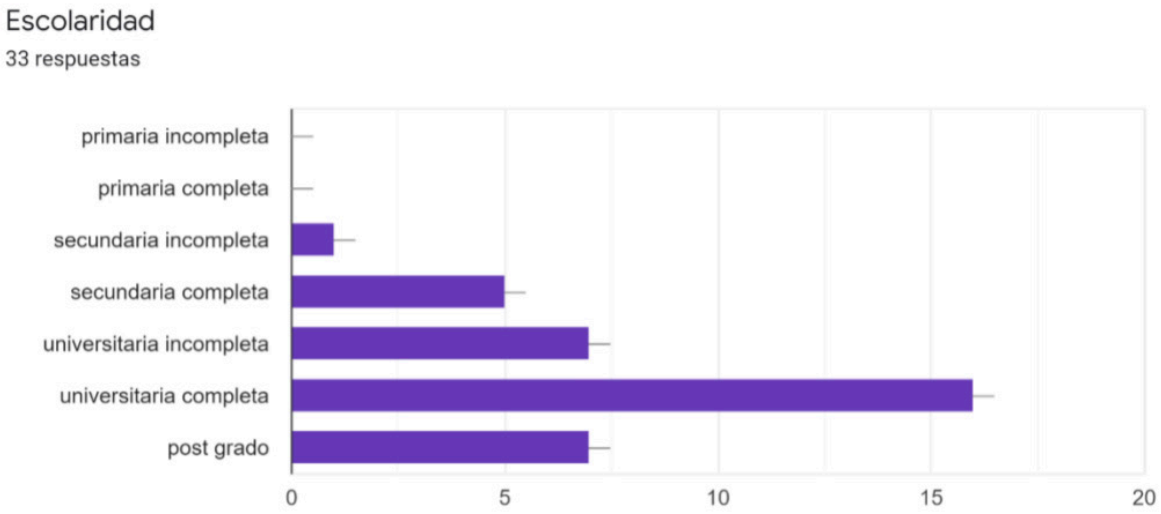

Figura 3. Escolaridad. Fuente: elaboración propia.

Un factor importante relacionado con el acceso a la conectividad y el uso del Internet es la zona geográfica, sea esta urbana, rural o mixta, y los resultaron arrojaron que 21 personas (63.6%) residían en una zona urbana; 5 personas (15.2%) en una zona rural y 7 personas (21.2%) residían en una zona catalogada como mixta (Figura 4), reflejo un poco del acceso a las comunicaciones que tenía el país, el cual políticamente está dividido en 7 provincias, consideradas 4 de ellas urbanas y 3 rurales.

Pero las 7 provincias tienen cantones y distritos que se consideran mixtos, pues no tienen cercanía con cabecera de provincia y no se encuentran tan urbanizadas como los cantones centrales de San José, Alajuela, Cartago y Heredia, siendo que el 48% (16 personas) residen en San José (capital del país); el 21.2 % (7 personas) en la provincia de Alajuela; el 15.2% (5 personas) residen en Heredia, provincia reconocida por su mayor ubicación de zonas francas e industriales; el 9.1% (3 personas) en Cartago; el 3% (una persona) en la provincia de Puntarenas; el 3% (una persona) en la provincia de Limón. Estas últimas dos zonas costeras tienen puertos para cruceros y terminales aduaneras, y el 0% (ninguna persona) en la provincia más turística del país, Guanacaste. (Figura 5).

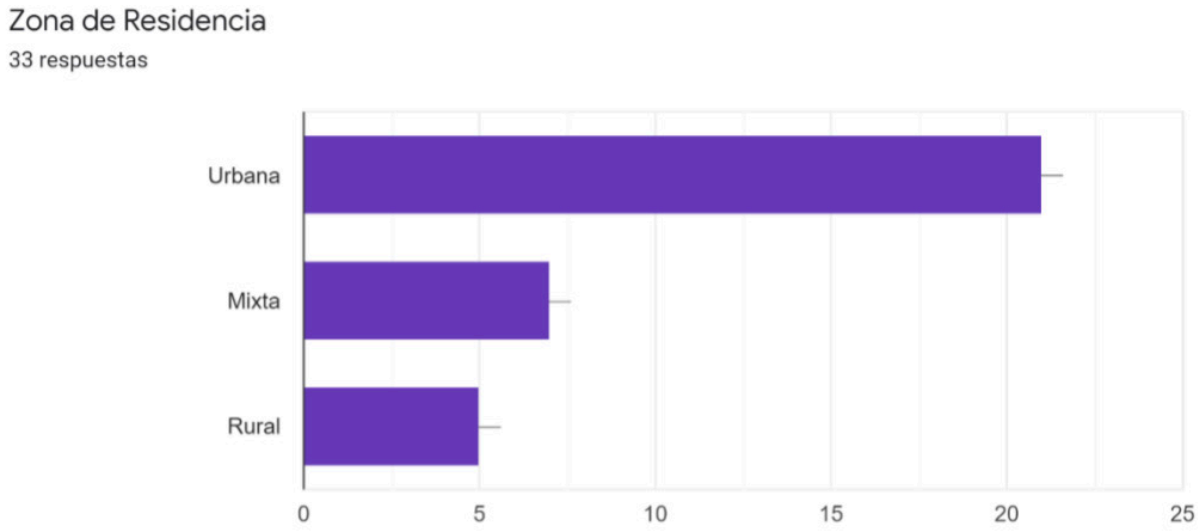

Figura 4. Zona de residencia. Fuente: Elaboración propia.

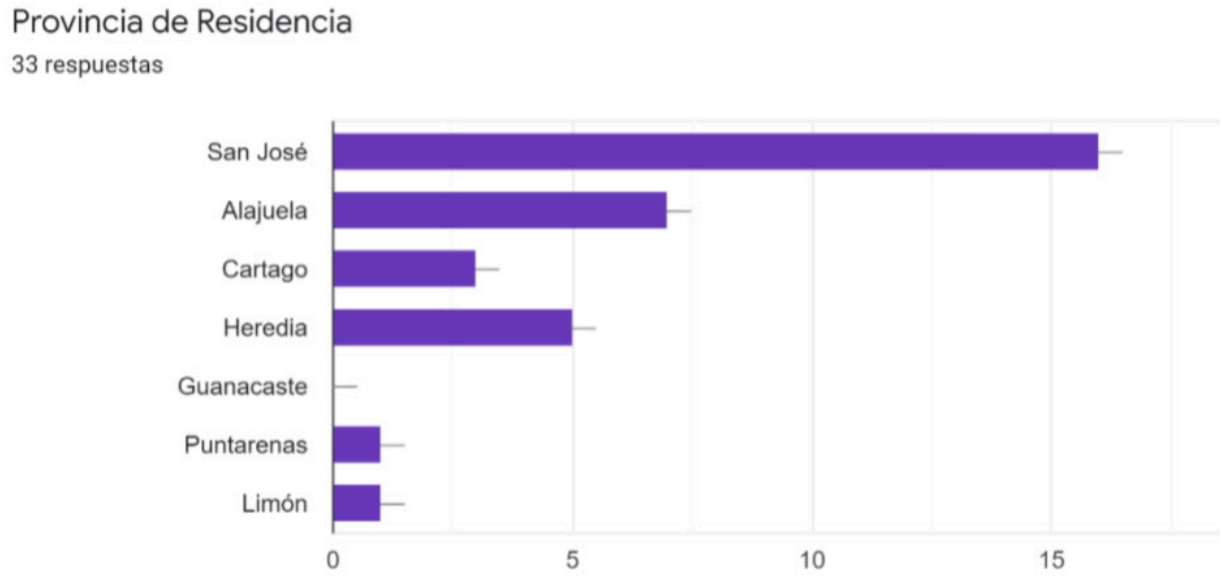

Figura 5. Provincia de residencia. Fuente: Elaboración propia.

Análisis de los datos y la Información obtenida

Conociendo entonces las características demográficas de las personas que accedieron a dicha encuesta, se analizan los datos sobre su conocimiento en el tema de estudio, siendo que un 57.6% sí indica que sabe lo que es el IoT, y un 42.4% no sabe al respecto. (Figura 6). Un alto porcentaje manifiesta su preocupación por la seguridad de sus datos y su privacidad en Internet, 90.9% vs. un 9.1%. (Figura 7).

Se evidencia que, a pesar de vivir en un mundo digitalizado y expuesto al Internet, se desconfía de este y del uso que se pueda dar de sus datos. Igual sentimiento se manifiesta ante la pregunta de si aceptaría y se sentiría seguro(a) de que sus datos estuvieran al alcance de todo el mundo: un 87.5% manifiesta que no, y un 9.4% que tal vez. Una persona no contestó. (Figura 8).

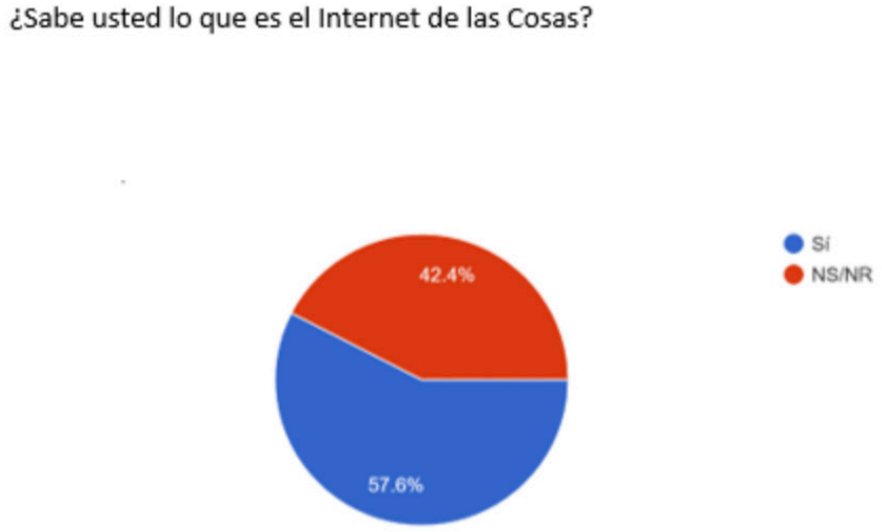

Figura 6. Pregunta: ¿Sabe usted lo que es el internet de las cosas? Fuente: Elaboración propia.

¿Está preocupado sobre seguridad y privacidad de los datos?

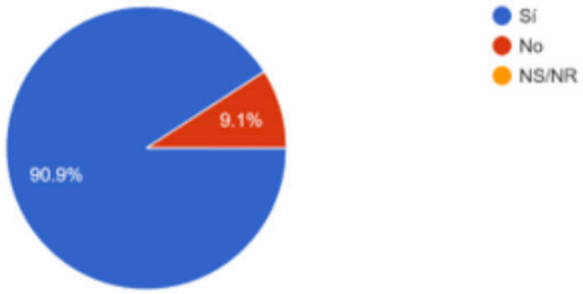

Figura 7. Pregunta: ¿Está preocupado sobre seguridad y privacidad de los datos? Fuente: Elaboración propia.

¿Aceptaría y se sentiría seguro de que sus datos estuvieran al alcance de todo el mundo?

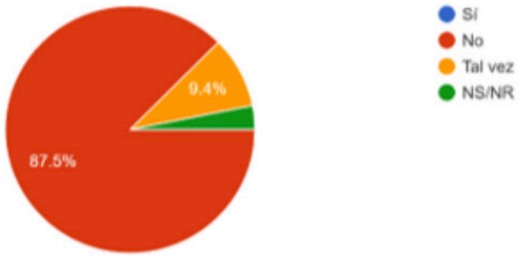

Figura 8. Seguridad ante el alcance de terceras personas a datos personales. Fuente: elaboración propia.

Al consultar sobre si el mundo está preparado para el IoT, la mayoría (45.5%) manifiesta que tal vez, un 33.3% indica que no, el 12.1% de la población consultada responde que sí y un 9.1% prefiere no responder. (Figura 9). Esto podría indicar que existe cierto grado de desconocimiento sobre el uso de esta tecnología que fue dada a conocer a finales del siglo XX, precisamente en 1999; es decir, desde hace un poco más de dos décadas, estamos rodeados del IoT y utilizamos dispositivos inteligentes y redes sociales.

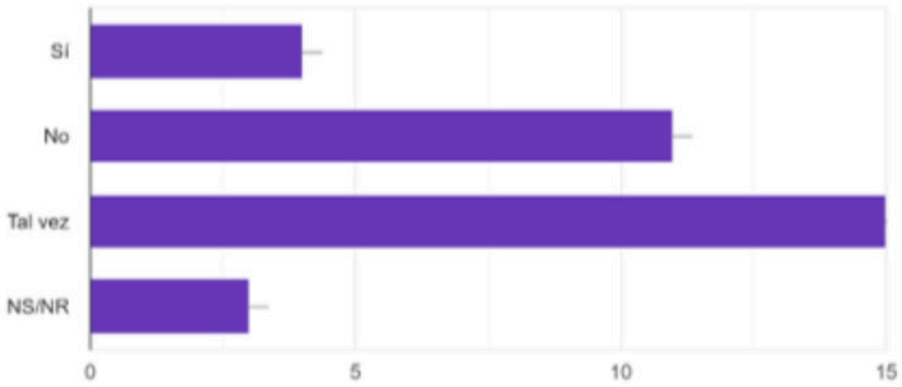

Figura 9. Preparación del mundo ante el IoT. Fuente: elaboración propia.

Con la novedad de los vehículos no tripulados como el auto Tesla, por ejemplo, se pregunta si aceptaría viajar en un vehículo autónomo, un 43.8% indica que sí, un 34.4% que tal vez, y un 21.9% que no (figura 10), evidenciando que el ser humano desea explorar y acepta dispositivos que faciliten la vida y la hagan un poco más cómoda, como lo es el hecho de viajar sin tener que conducir.

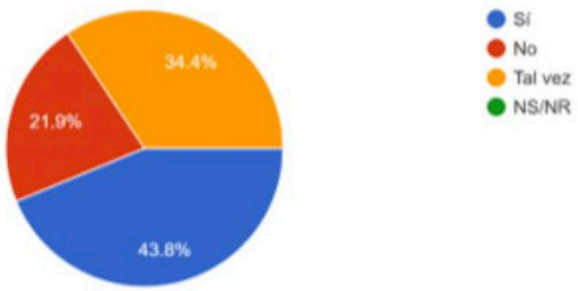

Figura 10. Aceptaría viajar en un vehículo autónomo. Fuente: elaboración propia.

Ante la pregunta sobre si considera que el IoT supone un cambio positivo o negativo, al ser una pregunta abierta, surge una variedad de respuestas agrupadas de la siguiente manera (Figura 11):

Once personas indican que el cambio es positivo.

Cinco personas manifiestan que no saben qué cambio traerá.

Dos respuestas en blanco.

Tres indican que depende del uso que se le dé.

Una manifiesta “en realidad, lo hacen ver como seguro, pero hay muchas personas que saben mucho del tema y hacen maldades”.

Tres personas consideran que puede tener ambos (positivo y negativo).

Una persona expresa que, si se sabe priorizar el cambio, es positivo.

Una persona asevera que, hasta cierto punto, puede ser positivo o negativo, si lo tomamos como herramienta de aprendizaje, pero si se toma solo para consultar y no aprender, entonces será una herramienta inútil.

Una persona manifiesta: “El internet siempre ha sido un arma de doble filo, así que no pienso que traiga consigo cosas muy buenas”.

Dos personas expresan que desconocen de qué se trata y que no tienen idea.

Dos personas indican que el cambio es nega

Una persona hace todo un análisis al indicar que “Ambos, si lo vemos desde el punto de vista de la privatización de la identidad es negativa cuando se vulnera la misma, pero, si lo vemos desde el punto de vista de la investigación forense, aportaría algunos insumos, en casos de desaparición y migración de personas dentro y fuera de Costa Rica”.

Esta gama amplia de respuestas evidencia que la mayoría de las personas piensa que el cambio será positivo, según el uso que se le dé. Pero hay un porcentaje pequeño de personas que desconfían mucho del uso y la utilidad de las aplicaciones, en especial del uso y los fines con que vaya a ser usado.

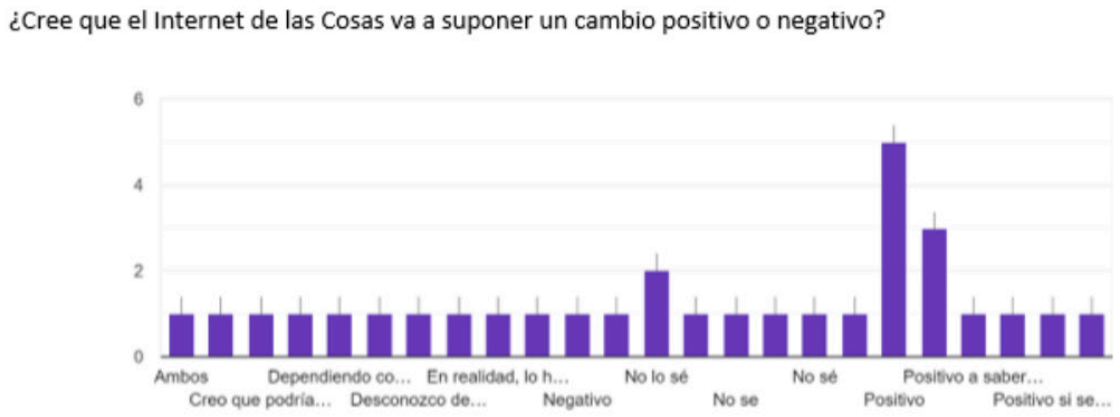

Figura 11. Representación gráfica ante pregunta abierta sobre el tipo de cambio que supone el uso del IoT. Fuente: elaboración propia.

Finalmente, dentro de la población que colaboró con el llenado de la encuesta, un 81.8% desea ampliar sus conocimientos al respecto, un 12.1% indica que tal vez y un 9.1% manifiesta que no desea ampliar sus conocimientos en el tema (Figura 12), siendo esto un indicador de que el tema es de gran actualidad. Pero también tiene aspectos de vulnerabilidad que es necesario saber y hay que mantenerse actualizado al respecto.

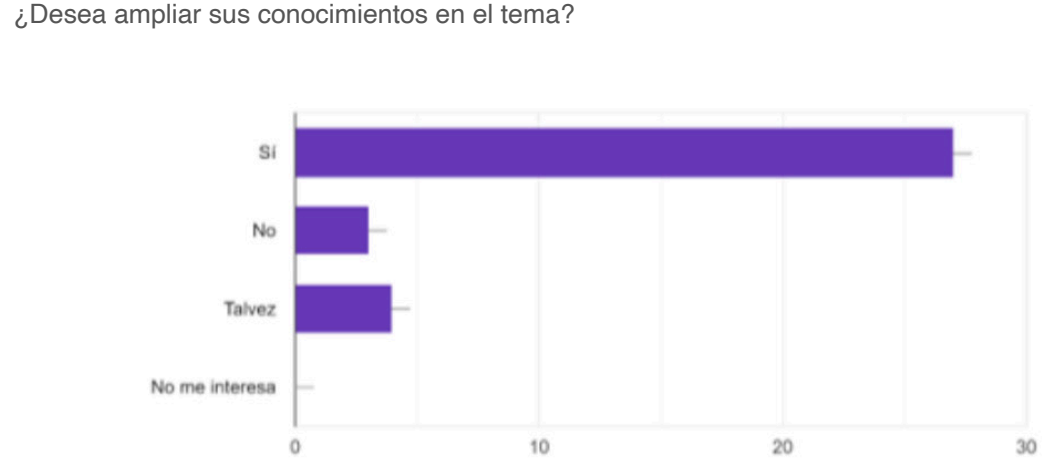

Figura 12. Ampliación de los conocimientos en el tema. Fuente: elaboración propia.

Aspectos teóricos sobre el Internet de las cosas

Si bien se relaciona el IoT con dispositivos móviles, no son solo un teléfono inteligente y unas redes sociales. Su aplicación puede llevar un sinnúmero de oportunidades para llegar a crear prácticamente un entorno inteligente. Así lo resumen Liñán Colina *et al.* (2015, p. 2):

> Partiendo de una compleja red que conecta millones de dispositivos y personas en una infraestructura de multi-tecnología, multi-protocolo y multi-plataforma, la visión principal de Internet de las Cosas (IoT), es la creación de un mundo inteligente donde la red, lo digital y lo virtual convergen para crear un entorno inteligente que proporcione más inteligencia a la energía, la salud, el transporte, las ciudades, la industria, los edificios y muchas otras áreas de la vida diaria.

Fue en 1999 cuando se empezó a usar el término *Internet of Things* (IoT). El británico Kevin Ashton hizo una presentación en la multinacional Procter and Gamble (P&G) en donde explicó el uso de sensores conectados a Internet para automatizar la recogida de datos y su aplicación en la cadena de suministros, añadiendo etiquetas RFID (*Radio Frequency Identification*, más conocidos como códigos de barras). De esta forma, se evitaban retrasos y errores por manipulación del operador y, con este sistema, se podría hacer seguimiento en tiempo real de varios aspectos del producto, tales como su utilización, su vida útil, la necesidad de aprovisionamiento, su funcionamiento, entre otros. Esto se ve reflejado en una reducción de costos y un aumento de la productividad.

Por tanto, IoT nace como una forma de facilitar información de cadena de suministros, bienes activos de las empresas e inventarios en general. Pero luego se extiende a otros objetos o cosas, animales, personas, entornos o ambientes, parafraseando a Moisés Barrio (2018, p. 21): "[…] de este modo, el IoT incorpora la dimensión de cualquier cosa a las TIC, que ya ofrece capacidades de operación en todo momento y en cualquier lugar y transforma así objetos tradicionales (pasivos) en inteligentes (activos)".

Se da entonces un valor añadido a las personas usuarias finales al hacer referencia a una tecnología basada en la conexión de objetos cotidianos a Internet, los cuales intercambian, agregan y procesan información sobre su entorno físico.

Cuando se inició el recorrido por el Internet, las personas usuarias quedaban sorprendidas ante la posibilidad de establecer contacto con la gente o de obtener información de cualquier parte del mundo y en diferentes zonas horarias.

El siguiente paso en esta revolución tecnológica es conectar objetos inanimados a una red de comunicación. Liñán Colina et al. (2015, p. 4) indican al respecto:

> La visión que subyace a la Internet de las Cosas permitirá el acceso a la información no sólo a "cualquier hora" y en "cualquier lugar" sino también usando "cualquier cosa". Esto será facilitado con el uso de la WSN y etiquetas RFID para extender el potencial de comunicación y monitoreo de la red de redes, así como para incorporar capacidades de computación en objetos y actividades de uso diario como afeitadoras, zapatos, embalajes.

De esta forma, se visualiza como una estructura que ofrece servicios de aplicación que permitan que las ciudades, servicios de transporte, edificios, industria, salud y otros más sean inteligentes apoyándose en la tecnología de redes de sensores inalámbricos (*Wireless Sensor Network*, WSN). Se pretende que los sistemas y aplicaciones de la IoT estén diseñados para proporcionar seguridad, privacidad, integridad, confianza, transparencia, anonimato, entre otros de interés de la persona usuaria. Pero siempre hay potenciales riesgos de uso indebido de esta tecnología.

Actualmente, el Internet comunica no solo computadoras o dispositivos móviles inteligentes (teléfonos / tabletas), sino también incluye muchos otros tipos de cosas u objetos desde ropas tecnológicas (relojes, pulseras, lentes de realidad aumentada), pasando por electrodomésticos, por ejemplo: refrigeradores, aspiradoras, televisores, hasta elementos más grandes como automóviles y dispositivos de edificios, tales como cámaras de seguridad, controles de acceso, sensores de temperatura, puentes, autopistas e, incluso, ciudades enteras.

González Larín (*El Internet de las cosas y sus riesgos para la privacidad,* sin año) enlista las tecnologías de comunicación, según la aplicación, rango de cobertura, seguridad, tamaño de los datos, exigencia de energía y duración de batería:

> A. Wi-Fi (*Wireless Fidelity*): Realiza transferencia de datos a través de radiofrecuencia y permite conectar dispositivos compatibles que estén cerca geográficamente.
>
> B. Bluetooth: Es un estándar universal abierto para enlaces de radio de baja potencia, hace parte de las redes *Wireless Personal Area Network* (WPAN) que normalmente abarcan distancias máximas de 10 metros.
>
> C. Telefonía móvil: Comunicación inalámbrica a través de ondas electromagnéticas.
>
> D. RFID: Tecnología que, por medio de etiquetas de identificación, se pueden seleccionar a los dispositivos remotamente por medio de señales de radiofrecuencia y así almacenar información, para luego ser procesados por los sistemas de gestión.
>
> E. Zig Bee: Define una serie de protocolos para la implementación de redes inalámbricas de corta distancia y baja velocidad de datos.
>
> F. Z-Wave: Tecnología inalámbrica ampliamente utilizada en productos domésticos, tiene una cobertura de 30.5 m, y cada red puede incluir hasta 232 nodos.
>
> G. 6 Low PAN (IDv6 *Over Low Power Wireless Personal Area Network*): Está enfocado en dispositivos simples y, al utilizar IPv6, es el ideal para redes con un gran número de sensores (pp. 4-5).

Viendo esta variedad de tecnologías, podría entonces asomarse algún tipo de riesgo sobre la captación, almacenamiento y uso de los datos, incluso cada vez que ha habido “apagones” de redes sociales y de Internet a nivel mundial. Ha sido innegable el impacto en la cotidianidad colectiva, dejando en evidencia que muchos de los grandes fabricantes de estas tecnologías aún no toman la seguridad y vulnerabilidad con el cuidado que se merece, o bien, tal vez se les haya salido de las manos.

Para ensombrecer un poco el panorama, hay que añadir el aumento de los ciberataques y las técnicas de "hackeo" cada vez más sofisticadas, ya que, parafraseando a González Larín, un solo ataque con éxito a la red del Internet de las cosas podría llegar a afectar todos los objetos físicos que nos rodean y, en el peor de los escenarios, la integridad física de las personas.

La hiperconectividad facilita mucho a las personas usuarias, pero, al mismo tiempo, vulnera la seguridad de esa conexión, en especial, la vulnerabilidad que tiene que ver con las contraseñas que, en su gran mayoría, no son seguras, pues para evitar el olvido involuntario, se crean autorizaciones sencillas como, por ejemplo, secuencias de seis números seguidos, o bien, de palabras predecibles partiendo de nombres o apodos de familiares, facilitando las cosas al ingenio de las personas especialistas en ciberataques.

Entonces, según el tipo de *software* e, incluso, de *hardware*, las personas podrían cometer errores, y otras personas se aprovecharían de esa vulnerabilidad, por lo que si se pone en perspectiva la misma evolución de los dispositivos y de las circunstancias que mediaron su creación, hay vulnerabilidad, por ejemplo, con la creación de los teléfonos inteligentes (que son una oficina en la palma de la mano), no se previeron las estafas telefónicas.

Podría casi asegurarse que nadie previó que se hiciera un uso indebido de ese dispositivo y, por ende, las leyes y normativas también se vuelven obsoletas. Se debe hacer un análisis legal cibernético para poder crear un cuerpo normativo robusto. Aunque existan una Agencia de Protección de Datos y una ley con su debido reglamento al respecto, no aseguran por completo la protección de los datos sensibles de los y las habitantes. González Larín brinda un ejemplo:

> los datos de geolocalización recolectados por algunos de los llamados gadgets para vestir o los Smartphone, que se están enviando constantemente a un servidor en algún lugar del mundo, ya sea para indicar la ruta en la que el sujeto hizo alguna actividad deportiva o sugerir la mejor ruta para llegar a un destino; si esta información cayera en manos de un atacante, éste podría detectar las costumbres o rutinas de la víctima y así encontrar el momento justo para hacer daño, ya sea directamente a la persona o alguno de sus bienes cuando no esté presente, todo esto gracias a la localización exacta proporcionada por los dispositivos.

¿Entonces, cómo la Agencia de Protección de Datos puede proteger mis datos de geolocalización, si además se hacen públicos voluntariamente en todas las redes sociales?

Es aquí donde tanto los fabricantes, las personas usuarias y quienes legislan deben poner de su parte para que toda la información sea segura, no solo los datos sensibles de las personas, pues, con el ejemplo anterior, se desprende que no solo en la privacidad de los datos hay riesgo, sino también en todo lo que se pueda obtener a través de ello, por lo que la principal recomendación es cifrar todos los datos que se van generando. De acuerdo con la empresa Kaspersky, especialista en seguridad cibernética:

> el cifrado en ciberseguridad es la conversión de datos de un formato legible a un formato codificado […] Cuando se comparte información o datos mediante Internet, atraviesan una serie de dispositivos de red en todo el mundo que forman parte de la Internet pública. A medida que los datos viajan por la Internet pública, existe una posibilidad de que hackers la comprometan o roben. Para evitar esto, los usuarios pueden instalar software o hardware específicos para garantizar la transferencia segura de datos o información. Estos procesos se conocen como cifrado en seguridad de redes. (www.kasperrsky.com, 2022).

En relación con Costa Rica y el Internet de las cosas, la inteligencia artificial y el uso eficiente de las tecnologías emergentes, el Plan Nacional de Ciencia y Tecnología 2015-2021 para Costa Rica indica entre otros aspectos:

> El desarrollo se enfocará en aumentar la eficiencia de la ciudad, potenciando sus capacidades para convertir los recursos en bienestar social y económico a través del monitoreo, vigilancia y ajuste de sus parámetros de operación. Esta etapa tiene como elemento principal la instrumentación de la ciudad mediante el Internet de las Cosas para obtención de datos hacia la toma de decisiones de manera más temprana y precisa. El factor energético es un objetivo esencial para la consolidación de esta fase. (Micitt, 2015, pp. 268-303).

Si bien es cierto, en Costa Rica, se han dado algunos pequeños avances en la línea planteada, aún falta visión estratégica que posicione al IoT, o bien, a la inteligencia artificial (IA) como una herramienta para el desarrollo tecnológico del país, así como una cosmovisión en seguridad y prevención de riesgos relacionados, ya que la estrategia es importante y según John Vélez Vergara:

> la adopción generalizada de la IA por parte de los gobiernos de todo el mundo está afectando no solo el orden internacional entre los estados, sino también el orden político dentro de ellos. Lo que está en juego en el futuro de la IA está íntimamente conectado con la competencia duradera entre los sistemas políticos e ideologías autoritarias y democráticas. (Vélez Vergara, 2022, pp. 13).

Desarrollo

Para llegar a una conclusión y recomendaciones adecuadas, debe partirse desde el conocimiento de las personas sobre el tema, pues prácticamente casi todos los individuos han adquirido un teléfono inteligente.

Según la superintendencia de telecomunicaciones (SUTEL), hay más de 8 millones de líneas celulares inscritas (2018, crhoy.com) en un país, cuya población aún no supera los seis millones de habitantes. O bien, de acuerdo con el Instituto Nacional de Estadísticas y Censos (INEC), en el caso de un televisor inteligente, el 92.4% de los habitantes del país ven televisión y, de ellos, el 44.7% lo hace a través de una *Smart TV*, según la Encuesta Nacional de Hogares del año 2020.

Los sistemas operativos de estos dispositivos permiten bajar aplicaciones que hacen que, con un clic desde estos, se pueda controlar el sistema eléctrico de una casa, por ejemplo, encender las luces de la sala desde el trabajo para así aparentar que en casa hay alguien, o bien, llevar un monitoreo de la frecuencia cardíaca desde una pulsera digital conectada mediante Internet al dispositivo móvil, programar el televisor para que tal día de la semana a tal hora, se encienda y transmita la película de preferencia para los niños de la casa.

Pero, ¿se han adquirido todos estos dispositivos por moda o teniendo conciencia de que la activación, el almacenamiento y uso de estos datos podrían llegar a emplearse sin el consentimiento de la persona usuaria para ofrecerle cada vez más productos diseñados, según el estudio de sus preferencias de mercado?

Si bien es cierto, la vida de las personas que han obtenido cierta tecnología ha mejorado significativamente, sus datos quedan almacenados en bases de datos que no se sabe realmente quién las maneja y, por lo general, no existe un consentimiento informado expreso sobre el uso de estos.

Cada vez que se utiliza algún dispositivo móvil conectado a la Internet, la persona va dejando el rastro de su huella digital, pero no hay un uso consciente de ello, y son las mismas personas usuarias que, al tratar de proteger sus datos, más bien los exponen.

No hay una cultura cibernética del uso de las redes sociales, de los dispositivos móviles e inteligentes y de todo aquello conectado a la Internet, incluyendo las claves de las cerraduras de las puertas de la casa administradas a través de un teléfono celular, entre otros posibles ejemplos.

Para entender mejor el concepto de huella digital, Castro Ávila (2021, p. 6) lo explica muy bien de la siguiente manera:

> *Cuando hablamos de huella digital nos referimos al rastro de toda nuestra actividad en internet, en su gran mayoría, creado voluntariamente por medio de las publicaciones y la búsqueda de información que hacemos, los sitios web a los que entramos, las aplicaciones que utilizamos, los "clics" o "me gusta" que damos dentro de las redes sociales, los pagos en línea, la activación de nuestras ubicaciones geográficas…otra parte de esa huella digital se crea con rastros de los que ni siquiera tenemos conciencia; por ejemplo, para que los sitios web se muestren correctamente en cada dispositivo que usamos (computadora, tablet o celular), el navegador entrega cierta información (resolución de pantalla, sistema operativo, ubicación y configuración del idioma) a las páginas que visitamos o a las aplicaciones utilizadas.*

Es ahí cuando se comienza a ver la sustracción de imágenes de personas usuarias de Facebook que son usadas en perfiles falsos, o bien, se inicia una especie de suplantación de identidad para hacer creer a los contactos de estas personas que están interactuando con el dueño oficial del perfil y, mediante mensajes, logran obtener información como cuentas de correo, números de teléfono y hasta pines de seguridad.

Las y los delincuentes cibernéticos han encontrado diferentes maneras de esquivar los antivirus y otras estrategias de seguridad y han logrado cometer muchos ilícitos a través de *malware, ramsonware* y otros tipos de *software* "maligno", mediante páginas webs falsas que aparentan ser reales, correos electrónicos con remitente conocido o por medio de enlaces fraudulentos.

Este impacto de los y las cibercriminales enciende la luz de alerta sobre la preparación de los individuos, las empresas y el mismo Estado ante posibles ataques cibernéticos de impacto. Al respecto, Vélez Vergara (2022, p. 35) indica:

> *Las tecnologías de IA exacerban dos desafíos de seguridad y defensa nacional existentes: en primer lugar, la dependencia digital en todos los ámbitos de la vida cotidiana, aumenta las vulnerabilidades a la intrusión cibernética de todos los segmentos de nuestra sociedad: corporaciones, universidades, gobiernos, organizaciones privadas y los hogares de la población civil. En paralelo, nuevos sensores han inundado el mundo moderno. El internet de las cosas (IoT), los automóviles, los teléfonos, los hogares y las plataformas de redes sociales recopilan flujos de datos, que luego se pueden introducir en sistemas de Inteligencia Artificial que pueden identificar, dirigirse y manipular o coaccionar a la población o ciudadanos del común. En segundo lugar, las amenazas internas y externas desafían al Estado por debajo del umbral de la confrontación militar directa mediante el uso de ataques cibernéticos, espionaje, guerra psicológica y política e instrumentos financieros.*

Como puede apreciarse, voluntaria e involuntariamente, las personas entregan sus datos sin percatarse de la efectividad o no del manejo de estos, por lo que se debe tener en cuenta una serie de medidas de seguridad personales; entre ellas, el manejo de claves y contraseñas seguras.

Así mismo, la Agencia de Protección de Datos de los Habitantes (Prodhab) debería visibilizarse un poco más e instruir a la población en general en temas de seguridad digital. Esto es lo que debería hacer dicha agencia, entre otros aspectos, según la Ley de Creación de la Prodhab N.° 8968:

> 1. Velar por el cumplimiento de la normativa en materia de protección de datos, tanto por parte de personas físicas o jurídicas privadas, como por entes y órganos públicos.
>
> 2. Llevar un registro de las bases de datos reguladas por esta Ley.
>
> 3. Acceder a las bases de datos reguladas por esta ley, a efectos de hacer cumplir efectivamente las normas sobre protección de datos personales. Esta atribución se aplicará para los casos concretos presentados ante la Agencia y, excepcionalmente, cuando se tenga evidencia de un mal manejo generalizado de la base de datos o sistema de información.
>
> 4. Ordenar de oficio o a petición de parte la supresión, rectificación, adición o restricción en la circulación de las informaciones contenidas en los archivos y
>
> las bases de datos, cuando estas contravengan las normas sobre protección de los datos personales.
>
> 5. Promover y contribuir en la redacción de normativa tendiente a implementar las normas sobre protección de los datos personales.
>
> 6. Dictar las directrices necesarias, las cuales deberán ser publicadas en el Diario Oficial *La Gaceta,* a efectos de que las instituciones públicas implementen los procedimientos adecuados respecto del manejo de datos personales, respetando los diversos grados de autonomía administrativa e independencia funcional.
>
> 7. Fomentar entre los habitantes el conocimiento de los derechos concernientes al acopio, el almacenamiento, la transferencia y el uso de sus datos personales.

Pero no solo existe la Prodhab, el ente rector en telecomunicaciones, el Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones (MICITT), también ha emitido recomendaciones que al parecer no se han socializado entre la población e, incluso, en la mayoría de las instituciones gubernamentales tampoco.

Al respecto, dentro del Plan Nacional de Desarrollo de las Telecomunicaciones (PNDT)(2022-2027) v05 de noviembre de 2021v3 de dicho ministerio, se hace una referencia un tanto escueta sobre la estrategia en ciberseguridad. La cita siguiente no es un extracto, sino la estrategia como tal, tomada de la página web del MICITT:

> *La estrategia en materia de ciberseguridad data de 2017 y procura la búsqueda de acciones conducentes al aseguramiento de datos y la protección en línea en diferentes aspectos, considera la persona como prioridad, el respeto a los derechos humanos y la privacidad, la coordinación con múltiples partes interesadas y la cooperación internacional (MICITT, 2017a).*
>
> *Como parte del marco de acción, se consideran otros instrumentos de planificación, entre los que destacamos el papel del PNDT como impulsor también, a la par de esta Estrategia, de una seguridad cibernética en diferentes sectores.*
>
> *Por lo tanto, lo delineado en la Estrategia a nivel detallado, se considera como un punto de partida para el PNDT en materia de seguridad cibernética y los retos que esto representa para las diferentes poblaciones, desde las infraestructuras críticas, los servicios en línea, servicios financieros, las MiPymes, las poblaciones en condición de vulnerabilidad, entre otros, para las que se debe considerar transversalmente el tema en los ejes de la planificación sectorial con visión al 2027. (MICITT, 2021, p. 29).*

Por su parte, en el *Protocolo de ciberseguridad*, documento de 15 páginas emitido por este mismo ministerio en conjunto con la Comisión Nacional de Emergencias, se establecen cuatro ejes principales de acción: un eje preventivo, un eje detectivo, un eje correctivo y un eje de coordinación.

Cada uno de estos ejes tienen tareas que se consideran claves para la detección, prevención, corrección y coordinación en caso de que las instituciones sufran de ataques cibernéticos. Pero analizando cada paso que se debe seguir, se nota que es muy básico y no se tiene contemplado este tema como algo propio de la defensa y seguridad del país. Ejemplos de esto han sido los recientes ataques perpetrados contra varios ministerios e instituciones estatales del Gobierno de Costa Rica, dejando en evidencia un vacío en este tema.

Y es que no solo corresponde tener oficinas de tecnologías de la información y comprar antivirus, ya que las y los maleantes cibernéticos hacen verdadera inteligencia e investigación de cómo introducir estos ataques. Al respecto, John Vélez lo visualiza de la siguiente manera:

> El malware en la era de la Inteligencia Artificial será capaz de mutar en miles de formas diferentes una vez que se aloja en un sistema informático…el uso que se amplía de las capacidades cibernéticas de Inteligencia Artificial existentes hará que los ataques cibernéticos sean más precisos y personalizados, acelerarán y automatizarán aún más la guerra cibernética, permitirán ataques más precisos, más sigilosos y persistentes, y harán que las campañas cibernéticas sean más efectivas a mayor escala. (Vélez Vergara, 2022, pp. 48).

Por esta razón, la estrategia nacional de ciberseguridad debe ser tomada con la seriedad debida, y se debe proporcionar todo el presupuesto que sea necesario para salvaguardar de una forma adecuada y ética la información del Estado y de las personas que habitan este país.

Incluso, dentro del PNDT 2022-2027, se cita una publicación de la UIT (Unión Internacional de Telecomunicaciones) del año 2020, la cual textualmente indica:

> Dotar a la población competencias digitales, se requiere la participación de diferentes instituciones: las universidades has de desarrollar investigación y establecer requisitos; las instituciones gubernamentales deben elaborar políticas adecuadas; los centros de formación han de impartir una formación en materias de competencias digitales adecuada; y el sector privado y las organizaciones de la sociedad civil deben apoyar la adopción y el uso de las tecnologías digitales (UIT, 2020, p.V (MICITT, 2021, p. 56).

Es decir, cuando en el año 2020, ingresó la pandemia a Costa Rica debido al virus SarsCov2 que produjo la enfermedad COVID-19, se redactó una directriz para dotar a la población de competencias digitales, y lo irónico es que la educación a nivel general en el país fue la más inaccesible y desigual en mucho tiempo, debido a que una gran cantidad de personas estudiantes no tuvieron accesibilidad ni conectividad para llevar sus clases en línea en los centros educativos del Ministerio de Educación Pública a nivel de primaria y secundaria.

Aún hoy, no existe cobertura del 100% en educación digital, ni tampoco se cuenta con las frecuencias de la tecnología 5G de forma estatal, evidenciando esto que muchos lineamientos y normativas tan solo se redactan para cumplir con una cuota. Pero no piensan ni redactan para tratar temas de seguridad nacional y de interés público, ya que hay muy pocas personas que conocen o que tienen competencias digitales, según lo exige esta altura del siglo XXI.

Conclusiones

A pesar de que se percibe que el Internet de las cosas es algo de reciente data, el uso de dispositivos conectados a la Internet tiene poco más de 25 años de existir; aunque el término como tal se haya comenzado a mencionar desde 1999.

Por lo general, las personas usuarias sienten que la privacidad de sus datos es un asunto que no debería ser de dominio público. Pero son las mismas personas usuarias quienes no elaboran contraseñas robustas, no verifican los protocolos de seguridad del fabricante y publican todo lo que hacen, incluyendo su posición por geolocalización.

Pero también, las personas usuarias están en lo correcto al indicar que depende del uso que se le dé, el IoT puede llegar a causar mucho daño, especialmente cuando el ataque sucede a un nivel no tan personal, sino a uno un poco más global, como las caídas mundiales o regionales de los servicios de electricidad o de telecomunicaciones, pues los sistemas de defensa de cada país quedan muy vulnerables.

Así, como las personas no son tan educadas en los temas digitales, el Gobierno y las instituciones tampoco propician este tipo de educación que genere competencias digitales en toda la población. Además, las instituciones tampoco tienen verdaderas estrategias ni planes de contingencia en caso de ciberataques perpetrados por grupos criminales organizados.

A pesar de la creación de una agencia de protección de datos con su ley y su reglamento, no pueden proteger la totalidad de la información que cada dispositivo emana y almacena, ni la forma en que se hace uso de esta.

Si bien es cierto, el Ministerio de Ciencia, Tecnología y Telecomunicaciones ideó un Plan Nacional para el sexenio 2015-2021, prácticamente al finalizar dicho periodo, no hubo mayor avance en la realización de este, evidenciando mucho entusiasmo, pero una nula ejecución de los proyectos en este tema.

La accesibilidad y conectividad son algo que no tiene una cobertura país del 100% a pesar de que el informe de la SUTEL (Superintendencia de Telecomunicaciones) del 2017 arroja que hay más teléfonos celulares que habitantes en el país, por lo que también se debe realizar una estrategia de acceso a la tecnología en cada región del país, incluso liberar las frecuencias 5G.

De esta forma, se comienza a cerrar esa brecha tecnológica que impidió que, durante la fase de cierre de la educación presencial durante la máxima ola de la pandemia (2020-2021), muchos estudiantes no tuvieran acceso a una educación en línea adecuada.

La digitalización de casi todos los procesos diarios es la norma en prácticamente casi todas las empresas públicas y privadas y en la vida diaria de cada persona. Todo se tiene conectado a todo, pero no se presta atención a la seguridad digital, no se le da el debido seguimiento, tampoco está dentro de los planes políticos, ni se toma en consideración en las políticas públicas del país.

Se deja como encargado al ente rector en la materia de tecnología y comunicaciones, pero no se hace una estrategia nacional de ciberdefensa y ciberseguridad como un todo

dentro de la seguridad de la soberanía de Estado por parte del Ministerio de Seguridad. Por tanto, se sugiere que conforme una comisión de enlace entre ambos Ministerios (MICITT y MSP) para investigar y adoptar un verdadero plan preventivo de mitigación y contención en temas de ciberseguridad, especialmente luego de ver los estragos que se han suscitado con los ataques al Ministerio de Hacienda y a la Caja Costarricense del Seguro Social, desestabilizando, en parte, la gobernanza y la gobernabilidad de un país que ha sido muy lastimado políticamente en los últimos 30 años; pero con más decadencia política en los últimos 12 años.

Se requiere que, dentro de los equipos de trabajo para estructurar las estrategias a trabajar en estos temas cibernéticos, se cuente no solo con profesionales en Ciencias de la Computación y la Informática, las ingenierías y otras ciencias puras, sino que también se cuente con personas profesionales en Ciencias Criminológicas (Criminología-Criminalística), ya que pueden aportar ideas sobre la seguridad y la defensa de la soberanía nacional, no solo en los asuntos de protección civil, sino también en protección, valoración de riesgos e investigación de todo lo concerniente con los temas cibernéticos.

Se insta de forma vehemente la creación de planes de estudio en todos los niveles de la educación costarricense, para educar a la población sobre cómo ejercer su “cibernavegación” de una forma más consciente y responsable, para que así mismo adquiera las competencias digitales adecuadas para cumplir con los Objetivos de Desarrollo Sostenible y no dejar a nadie atrás, especialmente en los siguientes temas:

4. educación de calidad,

9. industria, innovación e infraestructura,

10. reducción de las desigualdades,

11. ciudades y comunidades sostenibles y

17. alianzas para lograr los objetivos.

Referencias bibliográficas

Barrio Andrés, Moisés. (2015). *Internet de las cosas*. Editorial Resus. Tomado de https://www.academia.edu/42124225/INTERNET_DE_LAS_COSAS_Mois%C3%A9s_Barrio_Andr%C3%A9s_2a_edici%C3%B3n

Castro Ávila, Mariela. (2021). *Para entender cómo ejercer una ciudadanía digital responsable*. Primera edición. San José, Costa Rica. Instituto de Formación y Estudios en Democracia. Tribunal Supremo de Elecciones.

González Larín, Yeisson Germán. Sin año. *El internet de las cosas y sus riesgos para la privacidad*. Universidad Piloto de Colombia. Tomado de http://repository.unipiloto.edu.co/handle/20.500.12277/2681

http://prodhab.go.cr/funciones/

https://latam.kaspersky.com/resource-center/definitions/encryption

https://www.inec.cr https://www.micitt.go.cr/pndt-2022-2027/

https://www.micitt.go.cr/wp-content/uploads/2022/05/PROTOCOLO-CIBERSEGURIDAD-MICCIT-ICE-CNE.pdf

Liñán Colina, Antonio; Vives, Álvaro; Bagula, Antoine; Zennaro, Marco; Pietrosenmoli, Emano. (2015). *El Internet de las cosas*. Tomado de http://wireless.ictp.it/Papers/InternetdelasCosas.pdf

Ministerio de Ciencia, Tecnología y Telecomunicaciones. (2015). *Plan Nacional de Ciencia y Tecnología.* Tomado de: https://micit.go.cr/sites/default/files/pncti-2015-2021.pdf

Rojas, Pablo. (2018). *Telefonía móvil en Costa Rica: hay casi 2 líneas celulares por persona. Informe de SUTEL sobre 2017*. Tomado de https://www.crhoy.com

Sin autor. (2010). *Historia de las redes inalámbricas*. Tomado de https://histinf.blogs.upv.es