DIÁLOGOS CIUDADANOS

INTELIGENCIA ARTIFICIAL, ÉTICA Y PARTICIPACIÓN CIUDADANA

INFORME | EJE 1

Videovigilancia y seguridad:

El ciudadano ante sus derechos digitales

Autores:

Berta Llos, Profesora asociada de Ciencias de la Educación de la UAB

Dr. Carlos Sierra, director de comunicación del CVC

Núria Martínez, técnica de comunicación del CVC

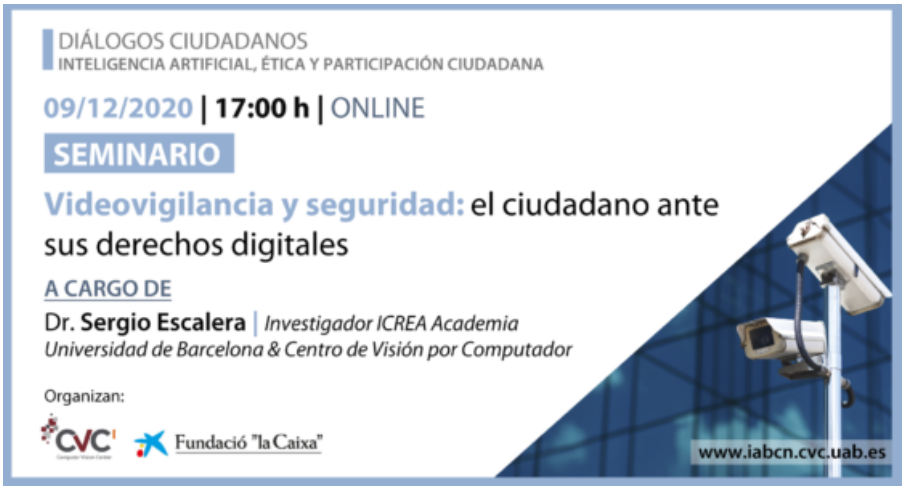
CVC Computer Vision Center

Fundació "la Caixa"

[09/12/2020] – SEMINARIO Y FOCUS GROUP

1) **Seminario (17:00 -18:00 h) –** Impartido por el Dr. Sergio Escalera

Enlace al seminario: https://www.youtube.com/watch?v=6pGX5RqiqY8&t=374s



2) **Focus group:** moderado por Berta Llos

- Participantes: 12 personas (6 mujeres y 6 hombres)
- Tuits de resumen del seminario (realizados por los participantes del focus group):

Las tecnologías de reconocimiento facial tienen muchas posibilidades .. y muchos riesgos! Tenemos que crear una buena regulación, y para ello necesitamos debate social.

Termino muy contenta de una presentación clara e interesante de Sergio Gracias, me quedo con #reconocimientodepersonas #biometría #cibervigilancia en proceso que necesita: #ética #regulación #sociedad #políticas #responsabilidades #transparencia

La clave está en la Regulación. Las posibilidades son infinitas, pero la posibilidad de error es preocupante

Lo más relevante: La importancia de una sociedad bien informada y una política capaz de garantizar el derecho a la privacidad.Qué he aprendido: Casos de uso interesantes (y socialmente buenos) de RF e IA

Tanto conocimiento y tanto desconocimiento!El conocimiento técnico está a años luz del conocimiento de la mayoría de la ciudadanía, que no tiene ni idea de los usos reales que se está dando a estas tecnologías

Inteligencia Artificial y seguridad humana: Un debate en el que los DDHH y la regulación van con retraso respecto de la velocidad del desarrollo tecnológico . Urge un debate social

Cada vez más nuestra información personal estará al alcance de las entidades públicas y privadas, es vital la unión y cooperación ciudadana para gestionar de forma justa y ética esta información

Buenas intenciones pero me ha sabido a poco toda la reflexión en torno a los riesgos de los sistemas de RF y cómo incorporar a la sociedad civil en el diseño de estos sistemas con un enfoque de Derechos Humanos.

Els experts en la tecnologia insisteixen diuen que manca regulació en relació a la videovigilància i que cal que usuàri/es siguin part del procés. Com ho fem?

Los algoritmos se equivocan pero muchas veces es porque las fuentes que tienen para aprender están sesgadas. ¿Es un problema con solución?

Nada es bueno o malo, sino el uso que se le da a ese algo

El Reconocimiento Facial es una tecnología ampliamente aplicada en nuestro día a día. No obstante, ¿cómo afecta esta tecnología a las personas más vulnerables?

Análisis del focus group:

OPORTUNIDADES DE DESARROLLO

**En general cuestan de identificar las oportunidades de la videovigilancia en específico, y se pone de manifiesto como los ejemplos dados a lo largo del seminario con Sergio Escalera que representaban una ventaja para el desarrollo, eran en general mecanismos de Inteligencia Artificial pero no de videovigilancia y seguridad.*

En términos de seguridad física puede ser beneficioso en diferentes ámbitos donde ya están utilizando, de hecho, algunos mecanismos: prevención de riesgos laborales, en comisarías o juzgados, lectores de matrículas, etc. También para la protección de espacios naturales/ seguridad medioambiental.

No por reconocimiento facial, pero como técnica de reconocimiento de imágenes se podría intervenir en zonas de conflictos armados, para hacer reconocimiento de terreno.

Con buena regulación y protocoles realizados desde la ética y transparencia, se podría estudiar la mejora de los derechos digitales y de hacer uso de la tecnología (en este caso de la videovigilancia y seguridad) para el soporte y desarrollo de los DDHH.

LÍMITES

Los sistemas de videovigilancia reproducen bases de datos con sesgos que implican discriminaciones de todo tipo, raciales, de género, etc. Si los equipos que trabajan con las bases de datos no tienen una mirada interseccional de la realidad, las bases de datos son discriminatorias y en consecuencia los propios sistemas de videovigilancia también lo son.

Vulneración de los derechos humanos. Los grupos vulnerables son los más afectados (Ej. campos de refugiados o control de fronteras). Se está entendiendo seguridad como seguridad física no como seguridad humana. Evidentemente a todos nos gusta sentirnos seguros, pero esta conceptualización genera que las decisiones que se toman están motivadas desde el miedo, hecho que va en detrimento de los DDHH sociales. Se reivindica que el pretexto de la seguridad no sea un mecanismo para vulnerar la privacidad ni la libertad de la ciudadanía.

La falta de regulación (a través de los comités de ética). Aunque existe el Reglamento General de Protección de Datos a nivel europeo, no quedan claros los usos de los datos, ni hay suficiente información. Peligro de una tendencia privatizadora de los datos públicos (Ej. Empresas del sector privado que proveen datos al sector público). Se consensua que los ciudadanos siempre se encuentran en desventaja, en términos de información, con relación a las empresas.

Hay cierto desconocimiento general sobre cómo funcionan los mecanismos de videovigilancia y seguridad, y sobre todo sobre por qué y cómo van a proteger o no tus datos. Falta de formación de ética en grados universitarios que estén relacionados con la Inteligencia Artificial (falta de formación en general a la sociedad desde jóvenes a técnicos profesionales, para que cada individuo pueda ser crítico).

Existe un vacío importante entre los discursos con relación a los mecanismos de videovigilancia y seguridad y las prácticas, la realidad. Por lo tanto, la incidencia directa que tiene en la ciudadanía

es un incógnito constante. En general está desinformada, y no tiene espacios en dónde pueda participar o decidir. Falta un trabajo pedagógico desde la academia y una tarea de transparencia por parte de los actores políticos. (Ej. debe garantizarse que las personas vigiladas sepan cuando se les está videovigilando).

La videovigilancia crea nuevas formas de poder que requerirán nuevas formas de control, y paradójicamente, aunque debería ser más vigilado quién más poder tiene, la práctica suele funcionar al revés.

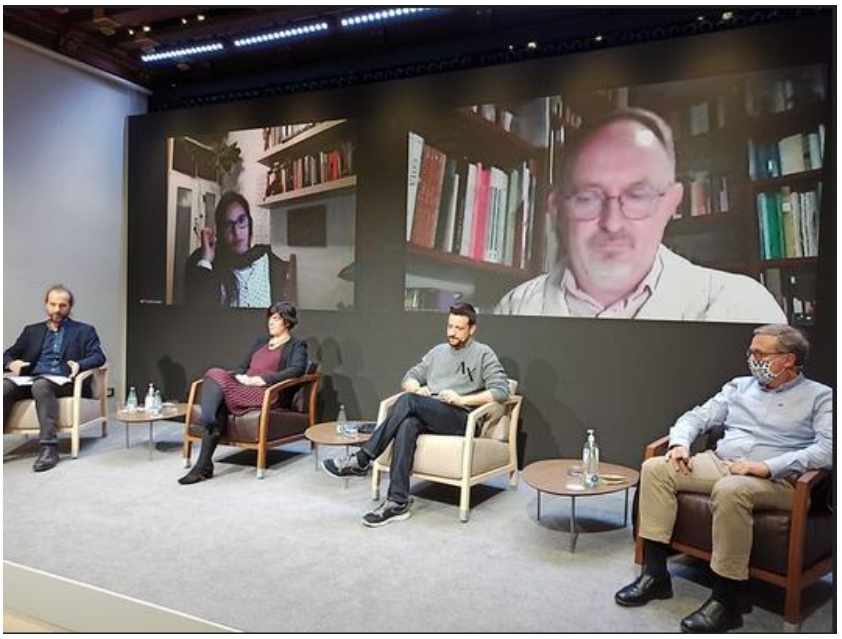
[15/12/2020] – DEBATE

Participantes:

- Dr. **Sergio Escalera,** investigador ICREA del Centro de Visión por Computador (CVC) y la Universidad de Barcelona (UB)
- Dra. **Carina Lopes,** directora del Laboratorio de Ideas de Sociedad del Futuro Digital al Mobile World Capital Barcelona
- Sr. **Joan Bautista Figueras,** responsable de la Unidad Central de Fotografía y Audiovisual en el Área de Identificación de la División de Policía Científica del Cuerpo de Mossos d'Esquadra.
- Dr. **Txetxu Ausín,** director del Grupo de Ética Aplicada del Instituto de Filosofía del CSIC (Madrid)
- Dra. **Lina María González,** coordinadora de proyectos en Derechos Humanos, empresas y seguridad humana y compra pública en NOVACT.

Moderado por: Dr. **Carlos Sierra**, director de comunicación del CVC.

- Biografías de los ponentes: http://iabcn.cvc.uab.es/videovigilancia-seguretat/
- Vídeo del debate: https://www.youtube.com/watch?v=WidwUgNPGK4&t=3s



CONCLUSIONES EJE 1

La Inteligencia Artificial ha progresado muy velozmente en los últimos tiempos, y la repercusión de sus avances está requiriendo un importante debate social, en este caso concretamente sobre aspectos relacionados con la videovigilancia y la seguridad.

Una de las principales conclusiones a las que se ha llegado después del trabajo de este primer eje es que **la tecnología per se no es ni buena ni mala**, por ese motivo el debate real se encuentra en los usos de esta. Se ha hecho evidente por algunas experiencias recientes, que un mal uso de los mecanismos, o incluso la falta de información sobre sus fines, ha llevado a situaciones discriminatorias para algunos sectores de la población. Por lo tanto, una primera necesidad e interés que se ha manifestado es **asegurar una forma más transparente de informar a la población sobre los distintos usos de la videovigilancia**, así como el manejo de los datos en cada uso, y aumentar con urgencia el trabajo para que los dispositivos sean más inclusivos.

Para lograr tal finalidad, hace falta no solo la voluntad, sino **una regulación** a partir de las administraciones públicas. Esta regulación debe garantizar la comunicación por parte de las instituciones a la población, pero también se identifica como necesaria la **educación y formación en todos los sectores de la sociedad**. En este sentido, se pone de relieve el insuficiente abasto del Plan Estatal de Inteligencia Artificial que, aunque supone un avance en relación con otros territorios para la protección de la ciudadanía, necesita aún de revisiones y corrección de sesgos. Paralelamente también se reconoce la "carta de los derechos digitales de la ciudadanía" como una buena práctica que debería ser más considerada por la administración y vincularla a organismos que tengan más capacidad de acción.

Otra de las conclusiones que ha resultado a partir de todo el proceso tiene que ver con la necesidad de que los mecanismos de videovigilancia sean **complementarios a la tarea humana**, es decir que sirvan de ayuda más que para substituir. Hay cierto consenso con la idea que cuando se utilizan los dispositivos no se pretende que estos hagan diagnósticos, y por lo tanto tiene que ser siempre la persona con su criterio quien tome las decisiones. En este sentido se han planteado diferencias entre reconocer e identificar, así como **videovigilar y videoproteger**, que pueden ser puntos de inicio para extender el debate y matizar los límites y oportunidades que ofrecen los dispositivos.

Finalmente, hay algunos consensos sobre ámbitos y espacios donde el uso de la videovigilancia es beneficioso, como en técnicas de prevención de enfermedades o de protección medioambiental. En cambio, en algunos otros casos, las opiniones son más diversas y se cuestionan aspectos como la posible vulneración de la intimidad, o los efectos del poder y control que puedan llegar a suponer, poniéndose de ejemplo escenarios de disidencia social. Otras cuestiones que quedan sin cerrar son las que tienen que ver con el financiamiento de los instrumentos de videovigilancia, o los intereses y relaciones entre grandes empresas y los gobiernos, por tanto, otra vez la relevancia y prioridad de la regulación y la transparencia.

Por ese motivo, una de las sugerencias más favorables que se ha identificado a partir de las interacciones ha sido la de **fomentar procesos participativos** en los que la inclusión y la no vulneración de derechos sean transversales, para que toda la ciudadanía tenga la

oportunidad de conocer e incluso ser parte de la toma de decisiones en los usos y fines de la inteligencia artificial, en este caso cuando se trate de videovigilancia y seguridad.

ENLACES DE INTERÉS

- **Crónica del debate** | *¿Videovigilar o videoproteger? El lenguaje importa, también en la Inteligencia Artificial*: http://www.cvc.uab.es/outreach/?p=2859

- **Vídeo del debate:** https://www.youtube.com/watch?v=WidwUgNPGK4&t=3s

- [EN LOS MEDIOS] **Carina Lopes: «Los algoritmos discriminan sobre todo a las mujeres»** | Artículo publicado en El Periodico | 14/12/2020 | Disponible en: https://www.elperiodico.com/es/entre-todos/20201214/algoritmos-mujeres-videovigilancia-discriminacion-11383592

- [EN LOS MEDIOS] **Txetxu Ausín: «La ética debe estar en el mismo diseño de la tecnología»** | Artículo publicado en La Vanguardia | 15/12/2020 | Disponible en: https://www.lavanguardia.com/vida/20201215/6124447/txetxu-ausin-etica-debe-diseno-tecnologia.html

ANEXO: **Preguntas y temas a tratar en el debate (extraídas del focus group del 09/12/2020)**

1. ¿Cómo van a garantizar que se informa muy claramente a las personas que están siendo filmadas, de forma que toda persona sea consciente de cuándo la están videovigilando? ¿Cómo van a evitar la adquisición indiscriminada de imágenes?

2. Formación a la ciudadanía: las empresas que lanzan las tecnologías deberían financiar también la formación de la ciudadanía para que pueda ejercer una opinión informada y participar en el debate social y político. ¿Qué ideas tienen al respecto? Esta formación no tiene por qué ser formal y aburrida, se puede desplegar de forma lúdica y participativa.

3. La formación debería incluir una pedagogía sobre las formas de poder que las innovaciones tecnológicas introducen en la sociedad. Propongo que se adopte el principio de que el nivel de vigilancia debe ser proporcional al nivel de poder: más poder requiere más vigilancia. ¿Están de acuerdo con esto? Me temo que en la praxis funciona al revés.

4. Hemos reflexionado que los algoritmos están sesgados porqué las personas tienen, en muchas ocasiones, un pensamiento discriminatorio. Entonces, ¿qué podemos hacer para que los algoritmos aprendan sin estos sesgos?

5. ¿Cómo podemos empoderar a la ciudadanía y como se garantiza la transparencia de los usos cuando se trata de videovigilancia?

6. ¿Conocéis cómo funcionan los mecanismos de videovigilancia en las fronteras? ¿Qué opinión tenéis al respeto?

7. ¿A quién se le compran las bases de datos? ¿Las empresas que producen tecnología dónde identifican esas Bases de Datos? ¿Dónde estaría el límite de los datos manejados por autoridades y los manejados por empresas privadas? ¿Cómo las personas pueden saber quién tiene sus datos y, por lo tanto, cómo logramos salir de esas BBDD?

8. Recientemente he escuchado a muchas personas comentar que, en su móvil, le aparecen anuncios personalizados de productos que no han buscado de manera activa pero sí han hablado del tema oralmente. ¿Hasta qué punto nuestros móviles “nos escuchan”?

9. A la Administración Pública: ¿Qué sabéis y qué se hace desde los comités de ética de vuestra institución con relación a la videovigilancia? ¿Todas las personas que trabajan en la institución los conocen, saben qué hacen? ¿Hay diversidad de profesionales en términos de género y etnia en vuestros comités? ¿Y en la institución?

10. A la Administración Pública: ¿Están las administraciones públicas construyendo espacios públicos de reflexión, con enfoque multidisciplinario e interseccional (por grupos social,

por etnia o género), sobre los mecanismos para regular y controlar la IA? ¿Cómo se está limitando la acción de las empresas en la creación de los mecanismos regulatorios? ¿Cómo se evita que la colaboración administración/empresa defienda el interés, la privacidad y los derechos de la ciudadanía?