Revista ADMINISTRACION PUBLICA y SOCIEDAD

ARTICULOS

Revista Administración Pública y Sociedad (APyS-IIFAP-UNC)
N° 14, Julio-Diciembre 2022 - ISSN: 2524-9568

Gobernanza ética de datos en la administración pública: Comentarios a partir del caso UPAD en Costa Rica

Ethical governance of data in the public administration: Comments from the UPAD case in Costa Rica

Jonathan Piedra Alegria[1]

Resumen: Este artículo examina el caso de la Unidad Presidencial de Análisis de Datos (UPAD) en Costa Rica, explorando los desafíos éticos y tecnológicos del uso masivo de datos en la administración pública. A través de un análisis hermenéutico de fuentes periodísticas y documentos legales, se abordan aspectos claves como el consentimiento informado, riesgos y beneficios, seguridad de datos, transparencia y confiabilidad. Se evidencia cómo la UPAD ilustra la necesidad de un enfoque interdisciplinario en la gestión ética de datos, promoviendo la transparencia y la participación ciudadana. Todo esto con la finalidad prevenir violaciones de derechos y garantizar un manejo óptimo de tecnología de análisis de datos en la Administración Pública. También se destaca cómo existe una línea delgada que separa el uso ético de datos personales para mejorar servicios públicos, de las consecuencias graves si dichos datos son mal manejados. La investigación concluye enfatizando la necesidad de regulaciones apropiadas, capacitación del personal, transparencia y rendición de cuentas para garantizar un uso ético y seguro de los datos personales en la Administración Pública.

Palabras clave:
Datos
gobernanza
Administración pública
consentimiento informado
privacidad

[1] Doctor en Filosofía. Máster en Filosofía Contemporánea, Máster en Derechos Humanos. Licenciado en Filosofía. Licenciado en Derecho. Docente e Investigador de la Universidad Nacional (Costa Rica). jonathan.piedra.alegria@una.cr. Grados: ID ORCID: 0000-0003-4532-4415.

Abstract: This article examines the case of the *Unidad Presidencial de Análisis de Datos* (UPAD) in Costa Rica, exploring the ethical and technological challenges of massive data use in public administration. Through a hermeneutic analysis of journalistic sources and legal documents, key aspects such as informed consent, risks and benefits, data security, transparency, and reliability are addressed. The UPAD case illustrates the need for an interdisciplinary approach in the ethical management of data, promoting transparency and citizen participation. All this with the aim of preventing rights violations and ensuring optimal management of data analysis technology in Public Administration. It also highlights how a thin line can separate the ethical use of personal data to improve public services, from the severe consequences if such data is mishandled. The research concludes by emphasizing the need for appropriate regulations, staff training, transparency, and accountability to ensure ethical and safe use of personal data in Public Administration.

Key words:
Data governance
Public Administration
Informed Consent
privacy

Introducción

El uso intensivo de datos se ha convertido en una práctica común en la sociedad moderna. Desde entidades bancarias hasta servicios en línea o aplicaciones de *streaming* recopilan y utilizan nuestros datos de manera directa o indirecta. Este uso de datos ha transformado la sociedad y nos brinda grandes oportunidades para mejorar tanto la vida pública como privada.

Sin embargo, también presenta desafíos éticos importantes. A medida que el uso intensivo de datos y tecnologías relacionadas evoluciona, también lo hacen las posibilidades de abusar de ellos. En el sector público, es indudable que la implementación de la Inteligencia Artificial (IA)

tendrá un impacto significativo en nuestras sociedades (Piedra, 2021). De hecho, se espera que dichas implementaciones tengan una gran influencia en la formulación de políticas públicas y en la automatización de procesos.

Como indica Jauregui (2021) “debemos tener en cuenta que los datos son el recurso más importante para una organización (privada, gubernamental o de cualquier sector), debido a la ganancia potencial que genera de una manera constante.” (pp.74). Si bien el manejo y el análisis de datos no es nuevo, ahora existe la posibilidad de procesar rápidamente enormes cantidades de datos (*Big Data*) y hacer correlaciones o predicciones utilizando conjuntos de datos dispares. Esto es importante ya que “el análisis de información permite hacer proyecciones sobre cuáles serán las necesidades más inmediatas, establecer estrategias adecuadas para prevenir situaciones que de otra manera, implicarían dedicar mucho tiempo tan sólo al análisis de la información” (García Vázquez, 2014, pp. 2), Sin embargo, es precisamente debido a esta recolección, manejo y análisis de datos (muchas veces privados) que surgen graves problemas sobre temas relacionados con la privacidad, la confidencialidad, la transparencia o la identidad (entre otros).

Colmenarejo (2017) señala con gran acierto que “este fenómeno está haciendo evolucionar el concepto de identidad hasta el punto de que necesariamente debemos considerar los cambios que esto implica respecto a nuestra relación ética con el concepto “ (pp. 68). Pero también surgen nuevos dilemas concernientes con una ciudadanía digital, nuestra identidad *on line*, así como en la forma en como una acelerada implementación de la IA puede reducir gradualmente la participación humana en la toma de decisiones. Este tipo de dilemas plantean dudas razonables respecto a los Derechos Humanos, la responsabilidad en la toma de decisiones o incluso en cuestiones más vastas como la actual transformación de la sociedad debido al uso intensivo de estos datos. La *smartificación* de la Administración Pública (Ramió, 2019) es un campo de estudio relativamente reciente en el que en algunas ocasiones no existe el análisis crítico que corresponde. Estas situaciones demandan estudios que nos permita abordar estos retos no solo desde un punto de vista legal sino también como desafíos éticos, en un sentido amplio.

Un aspecto particularmente importante se encuentra en la revolución (Jauregui, 2021) del uso de datos masivos en la Administración Pública. Con esta finalidad se tomará como caso paradigmático la creación de la Unidad Presidencial de Análisis de Datos (UPAD) en Costa Rica, con tal de analizar los elementos que rodearon su creación y mostrar cómo su implementación generó una serie de violaciones a la

privacidad, así como en la autonomía de los ciudadanos costarricenses. En un segundo momento, plantearemos algunas propuestas sobre el consentimiento en el uso de los datos y, finalmente, presentaremos algunos elementos necesarios para un manejo ético de los datos.

1. Crónica de una muerte anunciada: La UPAD.

El 17 de febrero del 2020 se publicó en Costa Rica el decreto Nº 41996-MP-MIDEPLAN (de ahora en adelante *Decreto*) que regularizaba la creación de la Unidad Presidencial de Análisis de Datos (UPAD). El principal objetivo de esta Unidad era la recopilación de información adecuada con tal de que el Gobierno pudiera tomar decisiones precisas relacionadas con la Administración Pública. Esto se lograría por medio de la generación de

> […] productos de información útil derivados del análisis de datos sobre asuntos de interés público, que permitan brindar insumos para fortalecer el proceso de toma de decisiones fundamentado en evidencia (Art.5.1 Decreto)

De manera general, la UPAD utilizaba técnicas de *Data Mining* con tal de "Aprovechar la enorme disponibilidad de datos generados por la digitalización y los avances en las tecnologías de la comunicación, así como el avance en las técnicas estadísticas y la ciencia de datos, para utilizarlas en la generación de insumos útiles para mejorar la calidad del proceso decisorio" (Art.5.2 Decreto)

La existencia de la UPAD se hizo oficial en febrero del 2020, pero en realidad había estado funcionando en Costa Rica desde el inicio de la gestión del presidente Carlos Alvarado en 2018. Inicialmente, se realizó una centralización de la información de varias instituciones públicas en una base de datos única, a pesar de que esta acción está explícitamente prohibida por ley. La información recopilada incluía datos personales de los ciudadanos costarricenses, aunque la naturaleza exacta de esta información sigue siendo incierta. Tanto así, que la única información sobre esto fue en primer lugar la que brindó la prensa al público, y posteriormente lo mostrado en un dictamen realizado por una Comisión Especial que se formó en la Asamblea Legislativa costarricense para investigar lo sucedido, por lo que solo existe un conocimiento parcial sobre los datos recopilados[2].

[2] El informe de la Comisión indica algunos de los datos que fueron recopilados. Por ejemplo, la Contraloría General de la Republica trabajó con asesores presidenciales para facilitar acceso a ciertos sistemas de datos. Asimismo, el Ministerio de Seguridad Pública compartió con la Presidencia una base de datos de aprehensiones de 2019. Se firmaron varios acuerdos con el Tribunal Supremo de Elecciones en 2016 y 2018 para acceder y

El 21 de febrero, sale a luz un reportaje en un conocido portal *on line* de noticias de Costa Rica (Chinchilla, 2020) en que se da conocer al público general por primera vez, la existencia de esta Unidad, así como el hecho de que recopiló datos confidenciales y sensibles de miles de ciudadanos. Debido al escándalo mediático de esta publicación, el presidente deroga el *Decreto*, cerrando de manera formal la UPAD. Como resultado de esta situación, comenzaron una serie de críticas sociales (incluso hubo reclamos formales de naturaleza penal de varios ciudadanos) y un juzgamiento político (se conformó una Comisión dentro de la Asamblea Legislativa para investigar lo sucedido), que provocó que en esa misma semana la Fiscalía General de la República, acogiera una serie de denuncias contra el presidente, así como contra el Director de Análisis de Datos de la Unidad[3] (que respondía exclusivamente al Presidente) y a los miembros de la UPAD, por los delitos de prevaricato, abuso de autoridad y violación de datos personales.

Esto provocó que por primera vez en la historia del país se realizara un allanamiento en la Casa Presidencial (en el cual se secuestró el teléfono celular y la computadora personal del presidente Alvarado). Para el día de hoy todavía se encuentra bajo investigación todo lo acontecido.

1.1 Tipos de Datos personales en Costa Rica

Según la *Ley de Protección de la Persona frente al Tratamiento de sus Datos Personales* (N° 8968) de Costa Rica, existen dos grandes categorías de datos personales: (1) Los datos personales (en sentido general) son aquellos que permiten identificar a una persona física. Es decir, cualquier dato que sirva para identificar a una persona directa o indirectamente, por medio de cualquier información referida a su identidad. Por ejemplo, el nombre, la dirección, número telefónico entre muchos otros. Estos a su vez se dividen en: (1.1) Datos personales de *acceso irrestricto*, como los que contienen las bases de datos públicas en general. Datos a los que cualquier persona puede acceder y (1.2) Datos personales de *acceso restringido*, que a pesar de que en ocasiones pueden encontrarse en algunas bases de acceso público, solo son de

utilizar sistemas de identificación y datos personales. La Superintendencia General de Entidades Financieras recibió una propuesta para intercambiar información del Centro de Información Crediticia con la UPAD, la cual fue archivada por incompatibilidades legales. Funcionarios de la Presidencia solicitaron información específica al Organismo de Investigación. El Banco Central compartió con la UPAD información económica, excluyendo datos confidenciales. El Ministerio de Planificación confirmó la creación de una nueva unidad de análisis de datos tras consultarlo con el Despacho Presidencial (Asamblea Legislativa de Costa Rica, 2020).

[3] El perfil del puesto no indicaba que fuera necesario ser especialista o tener algún conocimiento especializado en la protección de datos personales, sino solo “conocimiento tanto en el uso de técnicas de ciencia de datos como de ciencia política, administración pública u otras afines” (Art. 9 Decreto).

interés para la persona titular concreta (o en ciertos casos para la Administración Pública). En segundo lugar (2) se encuentran los datos sensibles, que en principio serían todos aquellos que impliquen información que pueda ser utilizada para discriminar o excluir a una persona. Ejemplos de este tipo de datos, serían la orientación sexual, la opinión política o las características socioeconómicas. En el caso de la UPAD, esta unidad recopiló y gestionó no solo datos de acceso restringido (1.2), sino además (2) datos sensibles, todos ellos a espaldas de la ciudadanía y la opinión pública. (Colegio de Abogados y Abogadas de Costa Rica, 2019; Asamblea Legislativa de Costa Rica, 2020).

2. Gobernanza (ética) de Datos (personales)

Desde la constitución de la UPAD se presentaron muchos elementos cuestionables. Consideremos, por ejemplo, las normas que aparecen en la Constitución Política de Costa Rica (como el derecho a la privacidad). Estas normas solo pueden modificarse en ciertos casos y siguiendo las formas que la misma Constitución indica. Formas dentro de las cuales no se encuentra un decreto presidencial, tal y como sucedió en este caso.

La situación que se vuelve mucho más oscura, ya que este tipo de decisiones administrativas antes de ser finalmente emitidas deben someterse a una revisión previa por parte del Departamento de Leyes y Decretos[4] con tal evitar alguna situación jurídica inadecuada. No obstante, en el caso que estamos comentando extrañamente no sucedió así (Herrera, 2020). En caso de que esto no fuera suficientemente irregular, el decreto se firmó en octubre y se presentó 5 meses después (Herrera, 2020). Una situación totalmente anómala para este tipo de actos.

Entrando propiamente en el fondo, uno de los elementos controvertidos del *Decreto* se encontraba en su artículo 7 ya que, en él, se menciona literalmente que "se brindará acceso a la UPAD a información de carácter confidencial con la que cuenten las instituciones públicas cuando así se requiera", violando claramente el principio que protege la privacidad[5] de los ciudadanos costarricenses. Así las cosas, la UPAD tenía

[4] En año 2018, el gobierno de Carlos Alvarado creó el llamado *Grupo de Apoyo Legal Presidencial* (GALP) que en apariencia si revisó el acuerdo que daba origen a la UPAD. Las características y la finalidad que diferencian este *Grupo de apoyo legal*, del *Departamento de Leyes y Decretos* no son muy claras, tanto así que parece que *de facto* existe una duplicidad de funciones entre ambas. Algunos diputados de ese momento incluso denominan a este *Grupo de apoyo,* como una estructura paralela: "El decreto UPAD estuvo ideado para dejarlos a ustedes en la oscuridad a propósito y, además, se creó una estructura paralela para brincarse todos los controles que precisamente hubieran evitado que se cometieran los errores que tuvo la firma y aprobación de este decreto" (Herrera, J. 2020)

[5] Artículo 12**:** Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su

potencialmente acceso a todos los datos personales de la población costarricense. Valga decir que, en estos casos, para hacer uso de este tipo de datos es necesario la aquiescencia por medio un consentimiento expreso (Art 5. Ley 8968[6]). No obstante, sobre cuál es el tipo de consentimiento que se necesita en estos casos existe todo un debate teórico, que se mantiene en la actualidad.

2.1 El Consentimiento Informado

El consentimiento informado (CI) es un proceso en el que los investigadores (o médicos) informan a los participantes (o pacientes) sobre un estudio con tal que puedan decidir de manera voluntaria si desean participar en una investigación o someterse a un procedimiento médico. Generalmente se ubica su origen en los Juicios de Nuremberg, como una respuesta a los experimentos que realizaron los científicos nazis, en contra de sus prisioneros en la Segunda Guerra Mundial. El así llamado *Código de Nuremberg* (1947) recoge como requisito indispensable (dentro de los principios que lo componen) el consentimiento voluntario de las personas a la hora de realizar un experimento científico que incluya la participación de seres humanos.

Sin embargo, fue hasta el año 1964 que la idea del CI se materializa en un documento de alcance internacional en la famosa *Declaración de Helsinki*. A partir de esa fecha, el CI ha aparecido en toda una gama de documentos éticos-no vinculantes, así como en textos legales vinculantes (nacionales e internacionales) en los cuales se subraya la importancia de la participación voluntaria e informada de las personas con tal de proteger, entre otras cosas, su autonomía, su capacidad de autodeterminación, así como la dignidad humana.

correspondencia, ni de ataques a su honra o a su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques (Constitución Política de Costa Rica).

[6] Artículo 5.- Principio de consentimiento informado. 1.- Obligación de informar. Cuando se soliciten datos de carácter personal será necesario informar de previo a las personas titulares o a sus representantes, de modo expreso, preciso e inequívoco: a) De la existencia de una base de datos de carácter personal. b) De los fines que se persiguen con la recolección de estos datos. c) De los destinatarios de la información, así como de quiénes podrán consultarla. d) Del carácter obligatorio o facultativo de sus respuestas a las preguntas que se le formulen durante la recolección de los datos. e) Del tratamiento que se dará a los datos solicitados. f) De las consecuencias de la negativa a suministrar los datos. g) De la posibilidad de ejercer los derechos que le asisten. h) De la identidad y dirección del responsable de la base de datos. Cuando se utilicen cuestionarios u otros medios para la recolección de datos personales figurarán estas advertencias en forma claramente legible. 2.- Otorgamiento del consentimiento. Quien recopile datos personales deberá obtener el consentimiento expreso de la persona titular de los datos o de su representante. Este consentimiento deberá constar por escrito, ya sea en un documento físico o electrónico, el cual podrá ser revocado de la misma forma, sin efecto retroactivo. No será necesario el consentimiento expreso cuando: a) Exista orden fundamentada, dictada por autoridad judicial competente o acuerdo adoptado por una comisión especial de investigación de la Asamblea Legislativa en el ejercicio de su cargo. b) Se trate de datos personales de acceso irrestricto, obtenidos de fuentes de acceso público general. c) Los datos deban ser entregados por disposición constitucional o legal.

El CI está compuesto por cuatro elementos principales: En primer lugar (I) La información. Esto quiere decir que los participantes deben recibir toda la información relevante. Esto incluye lo que se necesita para ser un participante, los riesgos y beneficios de su participación, la manera en cómo se usarán y protegerán los datos, etc. (II) Comprensión: La información es primordial pero no basta solo con recibirla apropiadamente. Los participantes deben comprender la información brindada. Esto significa que una parte clave del consentimiento informado implica asegurarse de que la información se comunique bien y que las personas la entiendan correctamente. (III). Voluntariedad: Los participantes no deben ser coaccionados, manipulados, persuadidos o engañados de ninguna forma. Debe existir un deseo genuino y una acción voluntaria que indique expresamente su pretensión de participar. (IV) Capacidad para tomar decisiones. El CI requiere que los participantes puedan sopesar los riesgos y beneficios, con tal de tomar su propia decisión sobre si quieren participar.

El consentimiento informado, *grosso modo*, es una manifestación del conocimiento y comprensión de una realidad concreta (i.e una investigación, un tratamiento, la creación de una base de datos etc.) e implica la expresión clara de un asentimiento que garantiza un proceso justo, así como una utilización ética de los datos. Precisamente por esto, es que el uso del CI trasciende al ámbito médico y se traslada a otros espacios en los cuales las personas puedan ser afectadas, como es el caso del uso de sus datos personales por terceros, y más específicamente en la situación que estamos analizando, por la Administración Pública.

Es importante aclarar que la utilización del CI no es solo un asunto meramente legal, sino que es un tema ético ya que los supuestos que subyacen en el CI representan mínimos éticos exigibles por la sociedad. De forma que el CI es una muestra del respeto por las personas y sus elecciones que existe en las sociedades democráticas contemporáneas. A pesar de esto, tal y como acertadamente lo indican Ballantyne & Schaefer (2018, pp. 3): “Cómo hacer que el consentimiento funcione en la era de los datos y cuando la falta de consentimiento es un motivo apropiado para bloquear la investigación son cuestiones éticas y políticas desconcertantes.”[7]

2.2 El consentimiento en la recolección de datos.

Esta situación desconcertante, es lo que ha provocado que en la literatura especializada existan discusiones sobre el tipo de consentimiento más adecuado para la recolección y la utilización de datos en las investigaciones científicas, ya que en muchas

[7] “How to make consent work in the age of data and when lack of consent is an appropriate ground for blocking research are vexing ethical and policy questions” Todas las traducciones son propias a menos que se indique lo contrario.

ocasiones, una gran parte de los datos obtenidos (i.e muestras biológicas) en estas investigaciones se utilizan sin consentimiento, especialmente cuando estos son utilizados en investigaciones secundarias (o derivadas de la principal) que no fueron informadas, ni mucho menos consentidas por los usuarios de los datos en una primera instancia. Si a esto le sumamos el incremento exponencial de la capacidad de las nuevas tecnologías, el uso masivo de los datos (por ejemplo, el *Big Data*), así como las técnicas para analizarlos y procesarlos, el tema del CI resulta un asunto de gran importancia para garantizar una utilización que siga parámetros éticos, especialmente en lo relativo a la gobernanza en la Administración Pública.

Para nadie es un secreto que existe un creciente interés de los Estados en aprovechar al máximo los beneficios del uso masivo de datos, así como las técnicas de automatización derivadas de ellos. No obstante, como ya hemos mencionado, esto plantea preguntas importantes que deben ser resueltas, especialmente cuando la Administración Pública, pretende utilizar estos datos para mejorar sus procesos internos o incluso, con la intención de definir políticas públicas. Una pregunta razonable que debería tenerse en cuenta es: ¿De qué forma se pueden proteger los intereses y la autonomía de los ciudadanos al usar sus datos personales? Las propuestas para resolver este problema son muy diversas, pero en el mundo de la investigación (biomédica particularmente) han surgido algunos puntos que nos pueden ser útiles para reflexionar sobre la gestión ética de datos en un sentido general.

2.2.1 Consentimiento amplio (*Broad Consent*)

En primer lugar, se ha planteado lo que se ha llamado: Consentimiento amplio (CA) el cual básicamente es un consentimiento alternativo (Maloy & Bass, 2020), relacionado con el almacenamiento, mantenimiento, así como el uso secundario de información privada o identificable para alguna investigación posterior o futura (que todavía no ha sido especificada).

Grosso modo, el CA es un tipo de CI (que debe cumplir ciertos requisitos adicionales[8]), con la particularidad de que se enfoca en el uso de información para una finalidad distinta a la especificada en la investigación principal. Usualmente el uso de este tipo de consentimiento se justifica por un tema pragmático, ya que es poco

[8] Por ejemplo, debe incluir una descripción general de los tipos de la investigación que se pueda realizar, y la información debe ser suficiente para que una persona razonable concluya que él o ella daría su consentimiento para los tipos de investigación previstos. También debe, entre otros elementos, identificar cada tipo concebible de investigación que podría llevarse a cabo no es posible ni deseable, por lo que amplias categorías de descripciones.

práctico, estar solicitando de manera constante un nuevo CI en cada nueva investigación en la cual pueda ser de utilidad de los datos. Por ejemplo, una muestra biológica obtenida en cierto momento puede ser utilizada muchos años después, por lo que la información del donante puede estar perdida o haber cambiado con el tiempo. Si se utilizara un CI nuevo en cada caso, esto no solo retrasaría de manera indefinida esta investigación secundaria, sino que además existe una presunción válida de que las personas no deseen ser parte de una nueva investigación, aun cuando esta se base en el interés público. Lo que el CA busca es permitir de manera legal y ética el uso de los datos obtenidos de manera adecuada en una investigación principal, en otra secundaria o alternativa.

2.2.2 Consentimiento dinámico (*Dynamic Consent*)

El consentimiento dinámico (CD) es una versión del consentimiento específico que tiene como característica principal ser "una interfaz interactiva personalizada que permita a los participantes participar tanto o tan poco como elijan y alterar sus opciones de consentimiento en tiempo real.[9]" (Kaye *et al*, 2014, pp. 142). Básicamente el CD es una nueva forma en cómo se presenta el consentimiento a las personas participantes o usuarias, por medio de plataformas tecnológicas basadas en la Web. La idea que subyace a esta propuesta es que el consentimiento en sus formas actuales (i.e un documento físico o un documento digital que debe ser rellenado por el usuario) es poco flexible, lo que refleja una versión estática del concepto de autonomía que no está acorde con la realidad investigativa ni del manejo de datos. Según Kaye *et al* (2014) la autonomía de una persona no se puede resumir a un único acto o decisión, sino que por el contrario implica una serie de decisiones y elecciones a lo largo de un período de tiempo. Es debido a esto, por lo que la propuesta del CD busca reflejar un "mayor respeto" por la capacidad de elección al permitirle a las personas-usuarias un mayor control y capacidad de decisión sobre su información personal a través de una plataforma interactiva en la que se puede decidir su uso, recibir actualizaciones en tiempo real de alguna modificación y si no se está de acuerdo retirar el consentimiento. Dicho de otra manera, el CD solicita un consentimiento específico para cada nueva investigación. En este sentido el CD es solamente una herramienta que facilita la obtención del consentimiento, y no una sustitución de los modelos tradicionales como el CI o el CA.

[9] "(…) an interactive personalised interface that allows participants to engage as much or as little as they choose and to alter their consent choices in real time".

2.2.3 Meta consentimiento (*Meta consent*)

Esta forma de consentimiento es:

> "un nuevo modelo de consentimiento (meta consentimiento) que combina los modelos amplio y dinámico, con opciones adicionales para el consentimiento general y el rechazo general. La idea es simplemente dejar que las personas elijan cómo desean dar su consentimiento para futuras investigaciones secundarias de datos recopilados en el pasado o de datos que se almacenarán en el futuro. Esto significa que el meta consentimiento es tanto retrospectivo como prospectivo."[10] (Ploug & Holm, 2015, pp. 2)

El Meta consentimiento (MC) es un procedimiento individual que toma en cuenta las diferencias e intereses personales. Al igual que el CD la información y las solicitudes se realizarían por medios electrónicos en los cuales se les notifique a las personas los tipos de investigación para las cuales se les solicita el consentimiento. Lo mismo pasaría en caso de la utilización de los datos personales. A partir de ahí, también se les informaría sobre el tipo de consentimiento que estarían otorgando (i.e un consentimiento específico, amplio, dinámico o si por el contrario rechaza algún elemento o todos) y sobre esta base se utilizarían los datos obtenidos en una primera instancia.

2.3 El consentimiento en la UPAD.

Como hemos mostrado, el tema del consentimiento en cuanto al uso y manejo de datos no es sencillo. Los diferentes modelos que se han propuesto plantean diferentes desafíos según el propósito que se busque. Sin embargo, existe un punto en común en literatura: sin importar el modelo que se escoja es necesario solicitar y obtener el consentimiento de alguna manera con tal de poder garantizar los derechos de las personas. Especialmente en casos como en la UPAD. Esto nos lleva sin lugar a duda a una serie de preguntas iniciales: ¿Se les pidió a los interesados su consentimiento en el momento de la recopilación de datos? En caso de que existiera la solicitud del consentimiento: ¿Qué tipo de consentimiento se les solicitó?, ¿En qué medida las preferencias de los interesados determinaron cómo se utilizarían los datos por parte de la UPAD?

Las respuestas a estas preguntas son bastantes desafortunadas. Para comenzar, no hubo ninguna solicitud, sobre ningún tipo de consentimiento para que la UPAD

[10] "a new model of consent—meta consent—that combines the broad and dynamic models, with additional options for blanket consent and blanket refusal. The idea is simply to let individuals choose how they wish to provide consent for future secondary research of data collected in the past or of data that will be stored in the future. This means that meta consent is both retrospective and prospective".

pudiera usar los datos de forma distinta a la cual fueron otorgados en un principio. Según el artículo 7 del Decreto derogado:

> Para el cumplimiento de las atribuciones constitucionales y legales del presidente de la República, las instituciones de la Administración Pública Central y Descentralizada deberán permitir el acceso a toda información que sea requerida por parte de la UPAD para el cumplimiento de sus fines y objetivos, salvo aquellos casos particulares donde la información sea considerada como secreto de Estado. Para ello, se les facilitará los accesos a los datos o brindarán los insumos de información de forma oportuna y en formatos que permitan su análisis y procesamiento estadístico, cumpliendo todos los estándares para una adecuada gestión de la información, de forma que se garantice la integridad, confiabilidad y seguridad de los datos.

Como vemos, no se necesitaba ningún tipo de autorización, consentimiento o siquiera conocimiento de los ciudadanos para que esta Unidad obtuviera cualquier tipo información personal. Si bien es cierto, como hemos visto en los ejemplos anteriores, la solicitud del consentimiento para todos los usuarios registrados en las bases de datos estatales representa un gran desafío, esto no es motivo para una propuesta tan poco ética como la que presenta el *Decreto*. La redacción del artículo parece indicar que, para evitar este problema, se eliminaron de manera absoluta no solo el consentimiento sino además cualquier tipo de información o notificación posterior que pudiera gestionar al menos parcialmente (y *a posteriori*) lo relacionado con el conocimiento sobre la forma en como la UPAD iba utilizar estos datos.

De hecho, en ninguna parte del documento se menciona la palabra consentimiento. Tampoco se menciona, el respeto a las personas, o la privacidad dentro de los principios que la deben regir (Artículo 4). Omisiones tan groseras, plantean dudas razonables sobre la finalidad con la que se iban a utilizar los datos personales. A pesar de que el *Decreto* indica que lo que se busca es “Generar productos de información útil derivados del análisis de datos sobre asuntos de interés público, que permitan brindar insumos para fortalecer el proceso de toma de decisiones fundamentado en evidencia”, no queda para nada claro la manera en cómo se logrará esto. Esta situación genera nuevas preguntas: ¿El uso que le dio o la iba a dar la UPAD a los datos difiere del consentimiento original? ¿El uso de los datos es novedoso y original? o ¿Es probable que sea coherente con las expectativas originales de los interesados? Pues bien, es fácilmente observable el hecho de que el acceso y la utilización de los datos personales que se encontraban en las bases de datos administrativas implicaba una

reutilización de los datos recopilados originalmente por el gobierno para necesidades operativas (crear productos de “interés público”) distintas a las cuales se recopilaron en primer lugar.

Así las cosas, que una persona haya brindado su consentimiento para que se recopilen sus datos como forma para acceder a un servicio determinado (i.e servicios de Hacienda) no implicaba que haya consentido que se utilicen o compartan posteriormente sus datos personales con otras instituciones gubernamentales, ni mucho menos con una unidad desconocida que respondía única y exclusivamente al presidente. Varios medios informativos comunicaron que la UPAD logró recopilar una gran cantidad de datos personales. Se menciona que obtuvo datos del Ministerio de Obras Públicas y Transporte (MOPT), el Instituto Mixto de Ayuda Social (IMAS), el Ministerio de Hacienda y del Ministerio de Educación Pública (MEP), entre otros (Carvajal, 2020). Actualmente no se sabe con certeza qué datos recopilaron exactamente ni con que fines fueron utilizados. Sin embargo, existen una gran cantidad de informes que muestran que se actuó de manera indebida, irresponsable y poco ética, poniendo en una situación de riesgo todos los datos recopilados, así como en una condición de vulnerabilidad a las personas dueñas de esos datos (Colegio de Abogados y Abogadas de Costa Rica, 2019; Asamblea Legislativa de Costa Rica, 2020).

Así, por ejemplo, los datos de Hacienda o los que pueden obtenerse del IMAS (relacionados con condiciones socioeconómicas particularísimas) son claramente de naturaleza sensible y su obtención por parte del UPAD fue producto de una violación flagrante a la privacidad de las personas, así como una transgresión a los derechos relacionados con la protección de datos (Asamblea Legislativa de Costa Rica, 2020). Frente a esto, se podría alegar que la información obtenida era anónima y de naturaleza confidencial ya que:

> […], también se brindará acceso a la UPAD a información de carácter confidencial con la que cuenten las instituciones públicas cuando así se requiera. Dicha información mantendrá en todo momento su carácter confidencial, independientemente del acceso que se le brinde a la UPAD. En estos casos, la UPAD y las instituciones deberán establecer acuerdos de gobernanza para garantizar un uso responsable y coherente de los datos que beneficie a los ciudadanos y fortalezca la confianza pública.

Sin embargo, eso no fue así. En una audiencia entre el presidente, algunos asesores de la UPAD y la Defensora de los Habitantes de ese momento, un asesor admitió que los datos no solo no eran anónimos, sino que los utilizaron con elementos de

identificación muy específicos como nombres y apellidos e incluso con direcciones personales[11] (Valverde, 2020). Incluso, cierta información obtenida por la Unidad presidencial fue utilizada para despedir a varios docentes del Ministerio de Educación Pública que participaron en una huelga nacional en el año 2018[12]. (Carvajal, 2020). De hecho, la información obtenida por la UPAD fue central para estos despidos, tanto así que el coordinador del equipo de asesores presidenciales confirmó que una de sus responsabilidades fue contribuir en la correlación de información entre el Ministerio de Educación Pública y Migración durante la huelga contra la reforma fiscal en 2018 (Muñoz *et al*, 2020), como parte de su labor para analizar el "impacto de la huelga". Lo cual, sin duda, no es un uso responsable y coherente de los datos que beneficie a los ciudadanos y fortalezca la confianza pública, tal y como lo señala el *Decreto* de creación de la UPAD.

Ciertamente, la situación pudo ser mucho más lesiva. Ejemplos de escenarios peores, los podemos encontrar en algunos países angloparlantes. *Verbigratia*, en el Reino Unido, el *Home Office* adquirió de manera secreta datos personales, relacionados con la nacionalidad de inmigrantes ilegales en condición de indigencia que duermen en las calles con tal de expulsarlos de Gran Bretaña (Townsend, 2017). Esto fue posible debido a que datos como el género, la nacionalidad o la salud mental fueron recopilados por trabajadores comunitarios, para posteriormente ser guardados en una base de datos llamada *Chain.* La finalidad de esta base de datos era fungir como un repositorio útil para las instituciones benéficas con tal de brindar ayuda a las personas sin hogar. Sin embargo, el gobierno de Reino Unido, la utilizó para fines nada caritativos o humanitarios.

Algo similar ocurrió en Estados Unidos en el mandato de Donald Trump, ya que oficiales de la *Oficina de Inmigración y Aduanas* utilizaron la información personal

[11] A pesar de que existe en Costa Rica la Agencia de Protección de Datos (PROHAD), la misma no ejerció ninguna labor de fiscalización, control o supervisión en este caso, tal y como lo hizo notar la Comisión Especial de la Asamblea Legislativa (Herrera, 2020, 19 marzo).

[12] La huelga de profesores en Costa Rica en 2018 fue parte de un movimiento más amplio llamado la "huelga contra el combo fiscal" que abarcó a una amplia gama de sectores de trabajadores públicos, incluyendo educadores, trabajadores de la salud y empleados de gobierno. La huelga comenzó en septiembre y se prolongó durante varios meses. El motivo de esta protesta fue la oposición a la reforma fiscal propuesta por el gobierno, oficialmente conocida como "Ley de Fortalecimiento de las Finanzas Públicas". Los sindicatos y los trabajadores estaban en contra de la propuesta, alegando que los cambios impondrían cargas impositivas desproporcionadas a la clase trabajadora y a los más pobres, mientras que los más ricos y las grandes corporaciones se verían relativamente menos afectados. Los maestros jugaron un papel significativo en estas protestas. En muchos casos, las escuelas cerraron debido a la huelga, lo que provocó tensiones significativas y debates sobre el impacto en la educación de los estudiantes. A pesar de las protestas, la reforma fiscal fue aprobada en diciembre de 2018.

contenida en una base de datos privada canadiense para ubicar, perseguir y deportar migrantes ilegales (Harwell, 2021). A pesar de que estos casos se presentaron a partir de la utilización indebida de bases de datos privadas, no es un tema que se resuma a ellas. Esto se puede ilustrar, de nuevo, en los Estados Unidos, puesto que también salió a luz pública, la manera en cómo fueron escaneadas sin consentimiento las fotografías de las licencias de conducir con la finalidad de deportar migrantes. Tanto así, que desde el año 2011 el FBI ha realizado 400.000 búsquedas en las bases de datos estatales y federales, sin ningún tipo de consentimiento (Escobar, 2019).

Casos como los anteriores nos muestran algunas maneras en como los Estados pueden acceder a información confidencial a través de bases de datos comerciales y públicas, sin estar autorizados a hacerlo. Además de estos problemas evidentes, estos incidentes son un símbolo de un problema aún más grande y a menudo subestimado: el poder, la intensificación de la vigilancia y el control a través de información privada. Esto se hizo evidente en el caso de UPAD, ya que como previamente mencionamos algunos de los datos personales incluidos en bases de datos gubernamentales fueron utilizados para despedir a personas que participaron en una huelga docente del año 2018 (Muñoz *et al*, 2020).

1.4 Riesgos y beneficios

Es evidente que el uso de grandes cantidades de datos en la Administración Pública puede generar importantes beneficios, pero también plantea graves riesgos. La complejidad y el volumen de datos superan con creces las capacidades de las herramientas de análisis tradicionales y de las habilidades humanas. Antes de implementar el uso de datos masivos y las tecnologías asociadas en la gestión pública, es necesario evaluar cuidadosamente y de manera realista los posibles riesgos. Se debe establecer claramente qué supuestos beneficios obtendrán los ciudadanos, la sociedad y, por supuesto, la Administración Pública con su uso.

Estos elementos deberían estar claros en el *Decreto* puesto que en él menciona que las TICs han “( ) aumentado de forma exponencial la capacidad de las sociedades para producir, almacenar, procesar y compartir datos. Se trata de una revolución digital que puede transformar el modo en que el Gobierno puede servir a los y las ciudadanas y cómo éstos a su vez pueden participar en el Gobierno.”

Sin embargo, en el *Decreto* no se especifica en ningún momento qué supuestos beneficios se producirán. Por el contrario, utiliza una narrativa ambigua que se limita a mencionar que la creación de la UPAD tiene como objetivo mejorar el “bienestar

de las personas" o "fortalecer la confianza pública". Además, se omite por completo la mención de los posibles riesgos. Solamente se menciona que se debe realizar un "análisis de datos de forma ética", lo que se podría suponer que es para minimizar los riesgos, pero la información contenida en el documento no permite especular con más precisión.

Lo que, si se puede decir, es que no se realizó una ponderación entre los riesgos y los beneficios. ¿Cuáles era los beneficios para personas en este caso? No es posible determinarlo con exactitud. Del Artículo 4 del *Decreto* se desprende que una finalidad era "mejorar la calidad de vida de la mayoría de las personas que habitan el país, sobre todo de los grupos más vulnerables", pero sin mayor aclaración al respecto. Como ya hemos mencionado, de lo que se conoce hasta ahora, se puede decir todo lo opuesto.

La falta de consentimiento no solo violó el Derecho a la privacidad de las personas, sino que también les impidió ejercer su autonomía, al decidir sobre el uso y manejo de sus datos personales. El consentimiento libre e informado es un aspecto fundamental en la recopilación de datos, y su ausencia en este caso resultó en una lesión directa a la autonomía de las personas. Además, la opacidad con la que se llevó a cabo el proceso, sin una adecuada comprensión o información por parte de las personas, agravó el problema ético que surgió de la recopilación de datos. Es importante considerar y mitigar estos problemas éticos para evitar daños a las personas y la comunidad.

Igualmente, se le produjo un daño indirecto a toda la población y particularmente a aquellos a los que sus datos fueron identificados. Como sabemos, los daños no se limitan a un perjuicio directo, también existen los daños indirectos.

> "El 'daño' puede ser directo o indirecto. El daño podría resultar de una desventaja o perjuicio que surja de la forma en que la organización con la que se comparte utiliza los datos; podría ser daño físico, si la exposición de ciertos tipos de información representa una amenaza para la seguridad de las personas." (Broad *et al*, 2017, pp. 21).

Solo la mera recopilación injustificada por parte de la UPAD, puso a todos los ciudadanos del país en una situación de vulnerabilidad. Tal y como indica Véliz (2022) la privacidad es tanto colectiva como personal. La utilización indebida de nuestros datos personales no solo no afecta de manera individual, sino que involucran a una gran gama de personas. Mis datos económicos, no solo me afectan a mí, también conciernen a mi pareja, familiares etc. La ubicación de mi residencia implica la de mis vecinos o la de mi comunidad. Mi número telefónico envuelve a todos con los que alguna

vez me comuniqué y así sucesivamente. “La privacidad es colectiva en al menos dos sentidos. Lo es no solo porque esos deslices por los que revelas tus asuntos privados pueden facilitar violaciones del derecho a la privacidad de otras personas coma sino también porque las consecuencias de la pérdida de privacidad se sufren a escala colectiva ( ) daña el tejido social como supone un riesgo para la seguridad nacional ( ) permite la discriminación y pone en riesgo la democracia” (Veliz, 2022, pp.95).
La protección de los datos personales es un asunto fundamental en las democracias. No puede existir privacidad (ni mucho menos intimidad) si nuestros datos son utilizados por el Estado (o por empresas privadas) de formas que desconocemos y que nunca hemos consentido.

> “La recopilación, el almacenamiento y el uso de datos deben estar diseñados para minimizar y gestionar los riesgos de daño. Los daños pueden ser físicos, económicos, psicológicos o reputacionales y pueden ser experimentados por individuos, comunidades u organizaciones. La anonimización (pseudonimización y desidentificación) ha sido la piedra angular para proteger de daños a los interesados individuales.”[13] (Ballantyne, 2018, pp.2).

Como vemos, aunque el potencial de la utilización de grandes volúmenes de datos es innegable para mejorar la gestión pública, los riesgos y consecuencias de su uso indebido son también significativos, especialmente en términos de privacidad y autonomía individual.

La ambigüedad en el Decreto, que no proporcionó claridad sobre los beneficios específicos que se esperaban ni abordó adecuadamente los posibles riesgos, subraya la necesidad de una mayor transparencia y rendición de cuentas en las iniciativas que involucran el uso de datos a gran escala. Esto implica un enfoque robusto y deliberado sobre los aspectos éticos, como el consentimiento informado y la minimización de daños, tanto directos como indirectos, a individuos, comunidades y organizaciones.

2.5 Seguridad de los datos.

Los peligros generados por la UPAD van más allá de la invasión de privacidad. Juntamente con la falta de consentimiento, que afectó la autonomía de una gran cantidad de personas, los datos personales obtenidos se almacenaron en dispositivos USB y

[13] “Data collection, storage, and use should be designed to minimize and manage risks of harm. Harms can be physical, economic, psychological, or reputational and can be experienced by individuals, communities, or organizations. Anonymization (pseudonymization and de-identification) has been the cornerstone of protecting individual data subjects from harm.”

computadoras personales de los miembros de la UPAD sin cumplir con las normas básicas de seguridad (Colegio de Abogados y Abogadas, 2019). Además, los expertos de la UPAD utilizaron la plataforma *Tableau* (tableau.com) para analizar y visualizar los datos sin tener en cuenta su falta de protección para información sensible, ignorando los estándares internacionales en cuanto a seguridad y poniendo en riesgo toda la información. Para empeorar aún más todo eso, los miembros de la UPAD no tenían formación en informática, ciencias de datos, protección de datos, ciberseguridad o ética de datos (Colegio de Abogados y Abogadas de Costa Rica, 2019).

Estas situaciones nos demuestran que no hubo ningún acercamiento técnico (ni cuidadoso) con respecto al almacenamiento y procesamiento de los datos adquiridos que permitiera preservar su integridad a largo plazo y la seguridad de estos. Su obtención no fue resultado de un proceso ético (también legal) que consiste en la cesión consentida de una manera rigurosa, verificable, objetiva, proporcionada y actualizada, que buscara mejorar la interoperatividad de la Administración Pública y calidad de vida de las personas.

Como se puede inferir, no solo no hubo un acercamiento ético en el ejercicio de la actividad de la UPAD, sino que tampoco existió una reflexión de este tipo en la constitución misma de esta Unidad. No hubo una adecuada preparación del personal, ni se siguieron principios elementales de seguridad. Se ignoraron los estándares de excelencia internacional (por ejemplo, guardar la información en USB personales), y hubo una serie descuidos elementales que fueron mostrados por los medios informativos. La única certeza de todo esto es que la UPAD no produjo ni un solo beneficio (de los que se tenga conocimiento) para ningún ciudadano. La ausencia de una gobernanza ética produjo graves vulneraciones en cuanto la privacidad de los datos personales, creó enormes riesgos en la integridad y la seguridad de esta información.

2.6 Transparencia

Desde luego que todo esto solo fue una continuación de la falta de transparencia con la que se gestionó todo. Desde la constitución de la UPAD hubo un secretismo y una falta de claridad que levantó sospechas, que posteriormente fueron confirmadas. La transparencia es un valor fundamental en la gestión ética de datos y es ampliamente reconocido como una herramienta para prevenir la corrupción y los actos ilegales en la administración pública. Su fundamento no es solo legal, sino además ético en tanto implica una relación dialógica basada en una difusión proactiva (Fox, 2007). En una relación de este tipo el Estado por un lado informa, explica y detalla el manejo de los

recursos públicos, así como de las decisiones que fueron tomadas (o que se van a tomar), mientras que, por el otro, los ciudadanos demandan el acceso a la información (Fox, 2007). Todo esto con tal de que pueden plantear dudas y propuestas, lo que promueve una mayor participación ciudadana, reforzando el carácter democrático que debe tener la Administración Pública.

"La transparencia es esencial para defender los beneficios de la ciencia de datos y evitar acusaciones de proyectos de big data nefastos y "secretos". También es un buen antiséptico para el comportamiento poco ético"[14]. (Drew C. 2016, pp. 7) Estas características han hecho que el tema de la transparencia en el tema de los datos personales haya sido regulado en documentos como el Reglamento General de Protección de Datos (2018) de la Unión Europea, la *California Consumer Privacy Act* (2018) o más recientemente la *Lei Geral de Proteção de Dados* (2020) en Brasil. En el caso de la UPAD no se elaboró (ni difundió) una información accesible, ni clara sobre los objetivos, y los procedimientos para el uso compartido de datos.

Por lo tanto, no existió un marco de gobernanza definido que les permitiera a los ciudadanos, tener elementos básicos para contextualizar la creación de esta Unidad. En ninguna parte del *Decreto*, ni en las posteriores declaraciones de las autoridades gubernamentales se aclararon las condiciones de acceso a los datos, el tiempo que iban a estar almacenados los datos, si se iban establecer límites para el anonimato o la confidencialidad de los datos; la comunicación o las formas en cómo se podía poner fin al uso compartido de datos por parte de los ciudadanos. Es necesario recalcar que no es simplemente un tema de buena gestión administrativa o de transparencia del actuar público, es un tema ético mucho más amplio que tiene que ver con la coherencia de las narrativas institucionales y la credibilidad de los órganos estatales, la congruencia de sus actos con valores y acciones democráticas. Pero especialmente con la idea de bien común y beneficio público.

Aun así, si asumimos, por el bien de la argumentación, que en la creación de la UPAD hubo una buena intención, es bien conocido que las opiniones de la gente sobre una acción gubernamental concreta dependen en buena medida de sus actitudes generales hacia la política en general y la probabilidad de que se tomen medidas como resultado. Por lo tanto, situaciones como estas crean descontento y dificultan el trabajo de la Administración Pública, no solo en cuestiones específicas, sino en sentido más amplio, ya que generan incertidumbre y un clima social pesado para otras propuestas, independientemente del tema.

[14] "Transparency is essential to make the case for the benefits of data science and to avoid accusation of nefarious 'secret' big data projects. It is also a good antiseptic for unethical behavior".

2.7 Confiabilidad

La confiabilidad es un aspecto fundamental que se considera en la evaluación de personas, organizaciones e instituciones. Se refiere a la cualidad de ser digno de confianza y se basa en la veracidad, consistencia y confiabilidad de los datos, sistemas de producción de conocimiento, integridad científica y estándares profesionales. Un alto nivel de confiabilidad es esencial para mantener un ecosistema de datos robusto y confiable. Cualquier abuso de confianza puede afectar seriamente la credibilidad y la reputación de las personas, organizaciones e instituciones involucradas, así como de toda una profesión o sector.

La UPAD, creada por el Gobierno costarricense durante el periodo 2018-2022, ha dejado un legado de desconfianza y desasosiego entre la población en cuanto a la recopilación y uso de datos personales por parte del Gobierno. Esta situación ha generado un clima de incertidumbre y ha provocado una percepción negativa hacia las verdaderas posibilidades sociales que puede ofrecer el uso de datos masivos en la gestión pública. Incluso, puede generar un exceso de protección que, en última instancia, puede ser contraproducente (Piedra, 2022). Por lo tanto, es vital establecer un marco de gobernanza ética que permita aprovechar de manera responsable el valor social de los datos para el bienestar de los ciudadanos y de la sociedad en general (Piedra, 2022).

En este sentido una gestión ética de los datos debe abordar:

> […] las preguntas apremiantes sobre las responsabilidades y obligaciones de las personas y organizaciones a cargo de los procesos, estrategias y políticas de datos, incluidos los científicos de datos, con el objetivo de definir un marco ético para dar forma a códigos profesionales sobre innovación, desarrollo y uso responsable, que pueden garantizar prácticas éticas que fomenten tanto el progreso de la ciencia de datos como la protección de los derechos de las personas y los grupos. Tres cuestiones son centrales en esta línea de análisis: el consentimiento, la privacidad del usuario y el uso secundario. (Floridi & Taddeo, 2016, pp.3)

Es decir, la gestión ética de los datos no implica únicamente el manejo en concreto de los datos, sino además una nueva visión sobre las políticas públicas y el actuar de las instituciones gubernamentales o administrativas.

Conclusiones

La UPAD es un recordatorio de cómo una mala gestión pública puede resultar en la violación de los derechos de los ciudadanos, incluso cuando se parte con buenas intenciones. Es necesario reflexionar cuidadosamente sobre los retos que se derivan del uso masivo de datos y evaluar si la tecnología propuesta es adecuada para el contexto específico, para evitar situaciones como las de la UPAD. Esta iniciativa invadió la privacidad de una gran cantidad de personas y puso en duda aspectos fundamentales de la democracia en nuestras sociedades.

Para evitar situaciones como estas en el futuro, es necesario un enfoque interdisciplinario en la gestión ética de datos en la Administración Pública. Se deben incorporar diferentes perspectivas y experticias, incluyendo especialistas en ciencia de datos, ciberseguridad, ética, filosofía, sociología, y trabajo social, entre otros. Esto requiere una revisión revolucionaria de la ética aplicada, para garantizar que la gestión de los datos cumpla con los derechos y valores fundamentales de los ciudadanos.

Por esta razón, es fundamental que se fomente la transparencia y la participación ciudadana en la toma de decisiones sobre cómo se utilizan los datos masivos en la gestión pública. Esto se puede lograr a través de la creación de marcos éticos que permitan la consulta y retroalimentación de los ciudadanos, así como la evaluación continua de los riesgos y consecuencias de los proyectos de datos. La idea no es limitar el potencial tecnológico, sino utilizarlo de manera responsable, con tal de aprovecharlo al máximo para el bienestar de la sociedad.

El caso de la UPAD en Costa Rica ilustra la importancia de un enfoque cuidadoso y especializado en la gestión ética de los datos en la Administración Pública, ya que la línea entre un uso adecuado (y ético) y un uso inadecuado puede ser muy fina en algunos casos. El uso de datos personales por parte de la Administración Pública puede ser muy efectivo para mejorar servicios públicos y mejorar la vida de la ciudadanía, pero también puede tener consecuencias graves si se utiliza de manera inadecuada o no se protege apropiadamente la privacidad de las personas. Por lo tanto, es importante que se implementen medidas efectivas para garantizar el uso ético y seguro de los datos personales en la Administración Pública, incluyendo la implementación de leyes y regulaciones adecuadas, la capacitación del personal, la transparencia, la rendición de cuentas en la recopilación y uso de datos personales.

Referencias

ASAMBLEA LEGISLATIVA DE LA REPÚBLICA DE COSTA RICA. (2020). “Informe de mayoría. Comisión especial investigadora sobre las posibles violaciones por parte del gobierno de la república al derecho a la intimidad de las personas, respecto a la obtención y manejo de sus datos personales (UPAD)” Expediente n°21.818. Recuperado de https://d1qqtien6gys07.cloudfront.net/wp-content/uploads/2021/06/Dictamen_21818INFORME-MAYORIA.pdf Consultado el 20 abril del 2023

BALLANTYNE, Angela; SCHAEFER, G. Owen. (2018). “Consent and the ethical duty to participate in health data research.” *Journal of Medical Ethics*, 44(6), 392–396.

BROAD, Ellen.; SMITH, Amanda; WELLS, Peter. (2017). Helping organisations navigate ethical concerns in their data practices. Open Data Institute.

CARVAJAL, Erick. (2020, 28 febrero). “Estas son algunas de las bases de datos que utilizó la UPAD.” *Crhoy.com*. Recuperado de https://www.crhoy.com/nacionales/estas-son-algunas-de-las-bases-de-datos-que-utilizo-la-upad/ Consultado el 20 abril del 2023

CHINCHILLA, Daniel. (2020, 21 febrero). “Alvarado crea oficina para obtener datos confidenciales de los ticos.” *Crhoy.com*. Recuperado de https://www.crhoy.com/nacionales/alvarado-crea-oficina-para-obtener-datos confidenciales-de-los-ticos/ Consultado el 20 abril del 2023

COLEGIO DE ABOGADOS Y ABOGADAS DE COSTA RICA (2019). *Informe técnico. Comisión ad hoc para el análisis sobre la creación de la unidad presidencial sobre análisis de datos.* Recuperado de https://www.abogados.or.cr/informeupad/ Consultado el 20 abril del 2023

COLMANEREJO, Rosa. (2017). *Una ética para Big Data*. Editorial UOC. Barcelona.

COLMANEREJO, Rosa. (2018). “Ética aplicada a la gestión de datos masivos” *Anales de la Cátedra Francisco Suárez*. Núm. 52 (2018), 113-129.

CONGRESSIONAL RESEARCH SERVICE (CRS) (2021) *Biometric Technologies and Global Security*.

DREW Cat. (2016) “Data science ethics in government.” *Phil.Trans.R.Soc.A,* 374: 20160119.

ESCOBAR, Luis. (2019, 8 julio). “Datos de licencias de conducir son usados para deportar a migrantes en Estados Unidos. Noticias”. *El Universo*. Recuperado de https://www.eluniverso.com/noticias/2019/07/08/nota/7415646/autorizacion-datos-licencias-conducir-seran-usados-deportar/ Consultado el 20 abril del 2023

FLORIDI Luciano, TADDEO Mariarosaria. (2016). “What is data ethics?” *Phil. Trans. R. Soc. A,* 374: 20160360.

FOX, Jonathan. (2007). “The uncertain relationship between transparency and accountability.” *Development in Practice*, 17(4-5), 663–671.

GARCÍA VÁZQUEZ, Mario. (2014). *Estrategia y Mercadotecnia de IBM Software*. Editorial IBM Impact, Nueva York, 2014.

HARWELL, Drew. (2021). “ICE investigators used a private utility database covering millions to pursue immigration violations.” *The Washington Post*. Recuperado de https://www.washingtonpost.com/technology/2021/02/26/ice-private-utility-data/

HERRERA, Juan José. (2020, 19 marzo) “Diputados señalan escasa utilidad de Prodhab en caso UPAD.” *Teletica*. Recuperado de https://www.teletica.com/politica/diputados-senalan-escasa-utilidad-de-prodhab-en-caso-upad_260575 Consultado el 20 abril del 2023

HERRERA, Juan José. (2020, 23 septiembre). “Decreto UPAD no fue revisado por departamento de Leyes y Decretos.” *Teletica*. Recuperado de https://www.teletica.com/politica/decreto-upad-no-fue-revisado-por-departamento-de-leyes-y-decretos_269070 Consultado el 20 abril del 2023

JAUREGI, Lander. (2021). “Big Data: la revolución de los datos masivos en la Administración Pública.” *Inguruak*, 71. 73-94.

KAYE Jane, WHITLEY Edgar A, LUND David, et al. (2015). “Dynamic consent: a patient interface for twenty-first century research networks.” *Eur J Hum Genet*, 2015; 23 (2): pp. 141–6.

MALOY, John. W.; BASS, Pat. F. (2020). “Understanding Broad Consent.” *Ochsner Journal*, 20(1), 81-86.

MUÑOZ, Daniela; POMAREDA, Fabiolo & MIRANDA, Hulda (2020, 25 febrero). “UPAD ayudó a identificar a docentes huelguistas que salieron del país.” *Semanario Universidad*. Recuperado de https://semanariouniversidad.com/pais/upad-ayudo-a-identificar-a-docentes-huelguistas-que-salieron-del-pais/ Consultado el 20 abril del 2023.

PIEDRA, Jonathan. (2021) “La Smartificación de la Administración Pública: apostillas críticas a partir del caso europeo”. *Cuadernos Salmantinos de Filosofía*

(Sección Monográfica: Filosofía e Inteligencia Artificial) Vol. 48, 2021, 235-250, ISSN: 0210-4857E-ISSN: 2660-9509 pp.235-250 DOI:10.36576/summa.144500

PIEDRA, Jonathan. (2022). “Decolonizando la Ética de la IA”. DILEMATA: *Revista Internacional de Éticas Aplicadas*. Nº 38, mayo.

PLOUG T, HOLM S. (2016). “Meta Consent - a flexible solution to the problem of secondary use of health data.” *Bioethics*, 2016; 30 (9): pp. 721–32. Recuperado de https://semanariouniversidad.com/pais/upad-ayudo-a-identificar-a-docentes-huelguistas-que-salieron-del-pais/ Consultado el 20 abril del 2023

PRESIDENCIA DE LA REPÚBLICA DE COSTA RICA (2020). *Decreto ejecutivo N° 42216 del 21 de febrero del 2020. Creación de la Unidad Presidencial de Análisis de Datos* (UPAD). Recuperado de http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?nValor1=1&nValor2=90591&nValor3=119449 Consultado el 20 abril del 2023

RAMIÓ, Carles. (2019) *Inteligencia Artificial y Administración Pública. Robots y Humanos compartiendo el servicio público.* Madrid: Los libros de la Catarata.

TOWNSEND, Mark. (2017, 2 diciembre). Home Office used charity data map to deport rough sleepers. *The Guardian*. Recuperado de https://www.theguardian.com/uk-news/2017/aug/19/home-office-secret-emails-data-homeless-eu-nationals Consultado el 20 abril del 2023

VÉLIZ, Carissa. (2020) *Privacidad es poder*. Datos, vigilancia y libertad en la era digital. Debate. España