UNIVERSIDADE DA CORUÑA

Facultade de Humanidades e Documentación

ESTUDO COMPARATIVO DE CÓDIGOS DEONTOLÓXICOS NO ÁMBITO DA XESTIÓN DIXITAL DA INFORMACIÓN E A DOCUMENTACIÓN. O CASO DE ESPAÑA, REINO UNIDO E ESTADOS UNIDOS

ESTUDIO COMPARATIVO DE CÓDIGOS DEONTOLÓGICOS EN EL ÁMBITO DE LA GESTIÓN DIGITAL DE LA INFORMACIÓN Y LA DOCUMENTACIÓN. EL CASO DE ESPAÑA, REINO UNIDO Y ESTADOS UNIDOS

COMPARATIVE STUDY OF DEONTOLOGICAL CODES IN THE FIELD OF DIGITAL INFORMATION AND DOCUMENTATION MANAGEMENT. THE CASE OF SPAIN, THE UNITED KINGDOM AND THE UNITED STATES

Alumno/a: **Santiago Rafael Sinde Pita da Veiga**

Director/a: **José Luis Tasset Carmona**

Grao: **Xestión Dixital de Información e Documentación**

Ano académico: **2022/2023**

Convocatoria: **Setembro**

Sinatura do/a alumno/a

Sinatura do/a Director/a

Resumo

Realízase unha comparativa entre os códigos deontolóxicos de España, Reino Unido e Estados Unidos, no ámbito da Xestión Dixital da Información e a Documentación, cos engadidos de extraer propostas de mellora para España e indicar en que aspectos coincide este país con Reino Unido e Estados Unidos. Os códigos deontolóxicos escollidos son os propios das profesións e ámbitos profesionais da rama máis característica do ámbito mencionado, cuxas profesións derivadas son, principalmente, científico/a de datos, *community manager*, *business intelligence*, produtor/a de contidos dixitais e enxeñeiro/a de datos. Os resultados obtidos non mostran códigos deontolóxicos senón, máis ben, manuais de boas prácticas, que inclúen principios de protección de datos, códigos éticos para a Ciencia de Datos, ética do Big Data e principios éticos de datos federais, entre outros aspectos, que mencionan cuestións como a transparencia á hora de tratar os datos, o respecto pola propiedade intelectual, a necesidade de explicar para que se recollen os datos, e o rumbo e a obxectividade nos algoritmos. Conclúese que, polo momento, non existen códigos deontolóxicos para os ámbitos profesionais da Xestión Dixital da Información e a Documentación, polo que resulta necesario seguir observando a evolución deste campo profesional.

Palabras chave: código deontolóxico; estudo comparativo; datos; Big Data

Resumen

Se realiza una comparativa entre los códigos deontológicos de España, Reino Unido y Estados Unidos, en el ámbito de la Gestión Digital de la Información y la Documentación, con los añadidos de extraer propuestas de mejora para España e indicar en qué aspectos coincide este país con Reino Unido y Estados Unidos. Los códigos deontológicos escogidos son los propios de las profesiones y ámbitos profesionales de la rama más característica del ámbito mencionado, cuyas profesiones derivadas son, principalmente, científico/a de datos, *community manager*, *business intelligence*, productor/a de contenidos digitales e ingeniero/a de datos. Los resultados obtenidos no muestran códigos deontológicos sino, más bien, manuales de buenas prácticas, que incluyen principios de protección de datos, códigos éticos para la Ciencia de Datos, ética del Big Data y principios éticos de datos federales, entre otros aspectos, que mencionan cuestiones como la transparencia a la hora de tratar los datos, el respeto por la propiedad intelectual, la necesidad de explicar para qué se recogen los datos, y el sesgo y la objetividad en los algoritmos. Se concluye que, por el momento, no existen códigos deontológicos para los ámbitos profesionales de la Gestión Digital de la Información y la Documentación, por lo que resulta necesario seguir observando la evolución de este campo profesional.

Palabras clave: código deontológico; estudio comparativo; datos; Big Data

Abstract

A comparison is made between the deontological codes of Spain, the United Kingdom and the United States, in the field of Digital Information and Documentation Management, with the added purpose of extracting proposals for improvement for Spain and indicating in which aspects this country coincides with the United Kingdom and the United States. The deontological codes chosen are those of the professions and professional fields of the most characteristic branch of the aforementioned field, whose derived professions are mainly data scientists, community managers, business intelligence, digital content producers and data engineers. The results obtained do not show deontological codes but, rather, good practice manuals, which include data protection principles, ethical codes for Data Science, Big Data ethics and federal data ethics principles, among other aspects, which mention issues such as transparency when dealing with data, respect for intellectual property, the need to explain what the data is collected for, and bias and objectivity in algorithms. It is concluded that, for the moment, there are no deontological codes for the professional fields of Digital Information and Documentation Management, so it is necessary to continue observing the evolution of this professional field.

Keywords: deontological code; comparative study; data; Big Data

ÍNDICE

1. Introducción

Los códigos deontológicos tienen una gran importancia en todas las profesiones, porque indican las normas honestas adecuadas que hay en ellas y porque, además, contribuyen a la definición del campo profesional, así como a su prestigio social. Son elaborados por los colegios profesionales, que son corporaciones de derecho público (instituciones que ejercen funciones público-privadas) que están capacitadas para proclamar y aprobar las normas que indican los deberes de cada profesión. Los códigos deontológicos deben ser cumplidos tanto por los miembros de estas corporaciones como por los profesionales a quienes van dirigidos.

En cuanto a la Gestión Digital de la Información y la Documentación, es un hecho que es un campo relativamente novedoso en todo el mundo. Está relacionado con el campo denominado "Información y Documentación", que tiene muchos años de historia y que abarca el ámbito de las bibliotecas, los archivos y los centros de documentación. La Gestión Digital de la Información y la Documentación se estudia en un grado universitario, siendo la Facultad de Humanidades y Documentación de Ferrol, perteneciente a la Universidade da Coruña, una de las facultades en las que se imparte. Este grado, especialmente el que se imparte en la facultad que se acaba de mencionar, es una modernización del antiguo grado denominado "Información y Documentación", que hasta hace poco se impartía en esta facultad y se había quedado obsoleto; a su vez, esa titulación procedía de los antiguos estudios denominados "Biblioteconomía y Documentación".

Debido a lo novedoso que es el campo de la Gestión Digital de la Información y la Documentación (y posiblemente también por otras razones), hay una inexistencia de estudios sobre los códigos deontológicos aplicados específicamente a ese campo. Concretamente, no existen estudios que expongan y comparen códigos deontológicos aplicados al campo mencionado, a diferencia del caso del campo "Información y Documentación". No ayuda a su aparición el hecho de que los códigos éticos y deontológicos vigentes en las asociaciones profesionales, como IFLA, ALA o SEDIC, no estén realmente actualizados, y que su contenido se adhiera más a una concepción de la profesión que está muy centrada en la idea clásica de Bibliotecario o Archivero, con el añadido de un poco de nuevas tecnologías.

Este trabajo intentará ser pionero en aportar información sobre el tema. Realizará, como refleja su título, un estudio comparativo de algunos códigos deontológicos existentes en España, Reino Unido y Estados Unidos, en el ámbito de la Gestión Digital de la Información y la Documentación. Para ello, en primer lugar, se indicará cuál es la metodología, los objetivos

y la hipótesis del trabajo. A continuación, se expondrá un marco de referencia, en el que se explicará lo siguiente: qué son los códigos deontológicos y cuáles son sus funciones, además de otros conceptos relacionados; qué son los colegios profesionales y qué función deontológica tienen; en qué consiste el Grado en Gestión Digital de Información y Documentación en la Universidade da Coruña y cuál es su situación en el resto de España; cuál es el proceso para elaborar un código deontológico; qué evoluciones hay en la deontología profesional, y cuál es la situación de los códigos deontológicos en el ámbito internacional. Posteriormente se expondrán, en un apartado llamado "Resultados", algunos códigos deontológicos de España, Reino Unido y Estados Unidos. Finalmente, en el apartado conclusiones, se indicarán las semejanzas y diferencias entre los códigos deontológicos de esos países, con la finalidad de proponer que las buenas prácticas desarrolladas en unos países se apliquen en los países en los que están menos desarrolladas; se indicarán las similitudes de los códigos deontológicos españoles con respecto a los otros dos países, y se extraerán propuestas de mejora para los códigos deontológicos españoles.

2. Metodología

La revisión bibliográfica es un pilar fundamental para elaborar este trabajo. Se han seleccionado obras en español y en inglés, cuya fecha de publicación pertenece, en su práctica totalidad, al siglo XXI. Algunas de las personas autoras de estas obras tienen un alto prestigio, medido por el nivel de veces que han sido citadas por otras personas en sus trabajos; es el caso de Stewart Clegg, Jeremy Bentham (filósofo clásico del siglo XIX, pero auténtico creador del campo de la Deontología y la codificación normativa), M.S. Schwartz, Juan Roger Rodríguez Ruiz, Carmen Verde-Diego y Sven Helin, destacando Stewart Clegg y Jeremy Bentham, que tienen un índice h altísimo. Estas personas han sido citadas en el marco de referencia, apartado en el que también ha sido citada la asociación "Unión Profesional", que es la asociación que agrupa a las profesiones colegiadas españolas.

Debido a la ingente cantidad de códigos deontológicos que hay en todo el mundo, se ha decidido escoger tres países: España, Reino Unido y Estados Unidos. La razón de la elección de España es que el autor de este trabajo es español y, además, está estudiando en una universidad española; concretamente, en la Universidade da Coruña. El motivo por el que se han elegido los otros dos países, Reino Unido y Estados Unidos, es el hecho de que estos países

tienen algunos de los códigos deontológicos más antiguos, prestigiosos y consolidados, en los ámbitos relacionados, directa o indirectamente, con la Gestión Digital de la Información y la Documentación. Los códigos deontológicos son los propios de las profesiones y ámbitos profesionales que guardan relación con la rama más característica (en el grado de la Facultad de Humanidades y Documentación de Ferrol también hay la rama de Archivos, Bibliotecas y Centros de documentación) de la Gestión Digital de la Información y la Documentación, cuyas profesiones derivadas serían principalmente: científico/a de datos, *community manager*, *business intelligence*, productor/a de contenidos digitales e ingeniero/a de datos.

Las citas y la bibliografía han sido procesadas con EndNote, y se ha utilizado el sistema de notas y bibliografía del estilo Chicago 17ª edición.

3. Objetivos e hipótesis

Objetivo general: indicar las similitudes y diferencias entre los códigos deontológicos de España, Reino Unido y Estados Unidos.

Objetivos específicos:

1. Indicar cuáles son las similitudes de los códigos deontológicos de España con respecto a los de los otros dos países.
2. Extraer propuestas de mejora para los códigos deontológicos españoles.

Hipótesis: el cambio de Información y Documentación a Gestión Digital de la Información y la Documentación hace necesaria una actualización de la deontología profesional más ajustada a los nuevos retos de la profesión, así como una actualización o incluso creación y nuevo establecimiento de los códigos deontológicos y/o profesionales de las profesiones emergentes vinculadas a este nuevo campo.

4. Marco de referencia

4.1. Los códigos deontológicos

4.1.1. Qué son

Un código deontológico es una guía de normas precisas para el profesional, cuyo objetivo es facilitar y orientar que se cumplan las normas morales que definen a una profesión determinada.[1] También se puede definir como un documento escrito, formal y diferente, consistente en normas morales que se usan para guiar el comportamiento de los empleados o de la empresa [2]; como el conjunto de creencias y valores que son considerados válidos por una organización profesional, que representan una manera de entender la profesión y orientan sobre cómo practicarla [3], y como la manifestación documentada, legal y formal de las expectativas que tiene una organización con respecto a los comportamientos éticos de sus empleados.[4] No pueden ser considerados, como códigos deontológicos, las normales morales que cada persona se autoimpone, las normas cívicas y de educación que la mayoría de la ciudadanía ha asumido, ni los códigos de conducta o ética empresarial.[5]

Los códigos deontológicos pretenden explicitar la dimensión estrictamente moral de una profesión, que son los comportamientos que se les exigen a unos profesionales, independientemente de que estén recogidos, o no, en las normas jurídicas.[6] Si los códigos deontológicos se incumplen y luego hay una difusión pública de ello, la persona o institución infractora recibe un castigo considerable; este es el caso de los comités de Ética de algunos

[1] Gonzalo Múzquiz Vicente-Arche, *La función deontológica de las organizaciones colegiales y su impacto económico y social*, Unión Profesional (Madrid, 2016), 30, https://unionprofesional.com/estudio/la-funcion-deontologica-de-las-organizaciones-colegiales/.

[2] Mark Schwartz, "The nature of the relationship between corporate codes of ethics and behaviour," *Journal of Business Ethics* 32 (2001): 248.

[3] Juan Roger Rodríguez Ruiz, *Ética profesional y deontología* (Universidad Católica Los Ángeles de Chimbote, 2015), 146.

[4] Jennifer Adelstein and Stewart Clegg, "Code of ethics: A stratified vehicle for compliance," *Journal of Business Ethics* 138 (2016): 55.

[5] Rafael Delgado-Alemany, Alicia Blanco-Gónzalez, and María-Ángeles Revilla-Camacho, "Códigos deontológicos: El rol de los colegios profesionales y las profesiones reguladas," *Revista ESPACIOS.ISSN* 798 (2020): 237.

[6] Rodríguez Ruiz, *Ética profesional y deontología*, 142.

colegios profesionales o instituciones, que publican las denuncias y resoluciones sobre las malas actitudes de un profesional o institución, lo que implica una sanción moral que suele tener un efecto grande.[7]

Desde la década de 1990, se considera que la formulación de códigos deontológicos limita las conductas indebidas, y que proscribe los comportamientos poco éticos cometidos por los miembros de las organizaciones. Estos códigos se representan como herramientas para gestionar riesgos, que limitan las oportunidades de cometer faltas éticas. Y es que la principal finalidad de los códigos deontológicos es, gran parte de las veces, minimizar el riesgo empresarial en vez de producir ética.[8] Cabe destacar que aún existe una gran incertidumbre sobre si los códigos deontológicos influyen, eficazmente, en el clima ético de las organizaciones.[9]

Los códigos deontológicos deben publicarse dentro de la empresa, o de la organización en cuestión, con el objetivo de que la conducta de los empleados se ajuste a los valores sociales y éticos que se han declarado; pero también deben publicarse de cara al exterior, con la finalidad de comunicar estos valores compartidos.[10] De hecho, el código deontológico no es solamente un instrumento interno, sino que es también un punto de referencia para las relaciones que hay entre la empresa, o la organización cuestión, y el mundo exterior. La aplicación de estos valores éticos, al comportamiento de los operadores de la empresa, provoca que esta aumente su reputación y mejore su imagen, con el objetivo de generar confianza en el exterior.[11]

Hay dos formas en las que un código deontológico puede influir en la alternativa que se ha elegido, a la hora de tomar una decisión con implicaciones éticas: la primera, es cambiando la percepción del responsable de la toma de decisiones sobre si una acción es ética o no; la segunda, es cambiando la manera en la que la persona responsable, de la toma de decisiones,

---

[7] Rodríguez Ruiz, *Ética profesional y deontología*, 143 - 44.

[8] Adelstein and Clegg, "Code of ethics: A stratified vehicle for compliance," 55.

[9] Sven Helin and Johan Sandström, "An inquiry into the study of corporate codes of ethics," *Journal of Business Ethics* 75 (2007): 263.

[10] Ennio Lugli, Ulpiana Kocollari, and Chiara Nigrisoli, "The codes of ethics of S&P/MIB Italian companies: An investigation of their contents and the main factors that influence their adoption," *Journal of Business Ethics* 84 (2009): 34.

[11] Mauro Zavani, *Il valore della comunicazione aziendale. Rilevanza e caratteri dell'informativa sociale e ambientale*, (Giappichelli Editore, 2000), citado en Lugli, Kocollari, and Nigrisoli, "The codes of ethics of S&P/MIB Italian companies: An investigation of their contents and the main factors that influence their adoption," 34.

valora los resultados que guardan relación con la selección de acciones éticas o no éticas.[12] En cuanto a quién es el ente que más se beneficia de los códigos deontológicos, este es la sociedad, ya que mediante ellos le resulta posible conocer qué puede esperar y exigir de los profesionales.[13]

4.1.2. Funciones

Las funciones de los códigos deontológicos son, fundamentalmente: [14]

a. El reconocimiento público de la dimensión ética de una profesión o actividad por parte de las personas que la realizan. Frente a una concepción simplemente tecnicista o de rentabilidad de lo que es ser un buen profesional, la aprobación de códigos deontológicos sirve para intentar revalorar la profesión por su dimensión moral, y al profesional por su ejemplaridad ética en su trabajo.

b. Especificar los contenidos morales específicos de una profesión, que son las normas y obligaciones que deben guiarla. Esta labor prescriptiva de los códigos deontológicos tiene varias finalidades. Por una parte, conocer los aspectos éticos de la profesión posibilita, a los profesionales, tener un punto de referencia para los problemas que se le presentan. Por otra parte, los códigos deontológicos sirven para combatir el relativismo y el subjetivismo, ya que exigen consensuar un marco común ético de principios, valores y normas en los que se base el diálogo y la discusión. Finalmente, los códigos deontológicos acumulan e incorporan contenidos mientras se actualizan, y así constituyen un acervo o patrimonio moral de la profesión, reflejando de esta manera el progreso ético de esta última. En este sentido, los códigos deontológicos construyen una sensibilidad hacia los valores éticos y profesionales, sobre los que ir formando la conciencia moral personal. Los códigos deontológicos, sin esta educación de la conciencia moral, no tienen sentido ni son eficaces, y la Ética profesional sería algo puramente teórico.

---

[12] John C. Lere and Bruce R. Gaumnitz, "Changing behavior by improving codes of ethics," *American Journal of Business* 22, no. 2 (2007): 9.

[13] Rodríguez Ruiz, *Ética profesional y deontología*, 149.

[14] Rodríguez Ruiz, *Ética profesional y deontología*, 146-49.

c. Los códigos deontológicos, en una profesión, ayudan a una persona a defenderse mejor de las presiones externas, es decir, de las ejercidas por el dinero, el prestigio, el poder y el estatus, y ayudan a que la profesión se haga valer y respetar frente a los condicionantes externos.

d. Permiten que una profesión realice su misión moral y dignamente. La formulación y adopción de códigos deontológicos implica el reconocimiento de que una profesión tiene que mejorar y continuamente vigilar las prácticas éticas de sus actividades.

e. La motivación de los códigos deontológicos debe ser convertirnos en profesionales mejores para servir mejor a la sociedad, esto es, potenciar el espíritu de servicio.[15]

4.1.3. Conceptos de Ética y Deontología

Según la RAE, la Ética hace referencia a "El conjunto de normas morales que rigen la conducta de la persona en cualquier ámbito de la vida. Igualmente es la parte de la filosofía que trata del bien y del fundamento de sus valores". Los códigos profesionales se rigen por la Deontología, que consiste en el conjunto de los deberes que rigen una actividad profesional, y la definición de la RAE es la siguiente: "Conjunto de deberes relacionados con el ejercicio de una determinada profesión".[16] La palabra "ética" procede de la palabra griega "ethos", que significa "carácter", "costumbre". En el lenguaje corriente, la Ética consiste en las normas bien fundadas que prescriben lo que los seres humanos deben hacer, normalmente en términos de derechos, justicia, obligaciones o beneficios para la sociedad.[17] Además, la Ética es un arte, un conocimiento que nace de la vida, cuyas herramientas son el conflicto y la decisión, las cuales necesitan la libertad, conciencia y responsabilidad de los actos que realizan las personas, para encontrar lo que es más conveniente para ellas.[18] No obstante, la definición de Ética más

[15] Niceto Blázquez, *Ética y medios de comunicación*, vol. 53700 (Biblioteca de Autores Cristianos, 1994), citado en Rodríguez Ruiz, *Ética profesional y deontología*, 149.

[16] Delgado-Alemany, Blanco-Gónzalez, and Revilla-Camacho, "Códigos deontológicos: El rol de los colegios profesionales y las profesiones reguladas," 231.

[17] Lugli, Kocollari, and Nigrisoli, "The codes of ethics of S&P/MIB Italian companies: An investigation of their contents and the main factors that influence their adoption," 33-34.

[18] Ángel García Fernández, "Ética y deontología," *Educación y biblioteca* 19, no. 159 (2007): 71.

aceptada es la ciencia del comportamiento moral, obtenida a través del análisis exhaustivo de la sociedad, que podría determinar cómo deben comportarse o actuar sus miembros.[19]

La Deontología es la rama de la Ética que fue ideada por Jeremy Bentham (1748-1832), que es considerado el padre de la filosofía utilitarista inglesa, en su obra "Deontología o Ciencia de la Moral" [20], y se define como la teoría del deber, o ciencia de los fundamentos del deber y las normas morales. Alberga varios mínimos obligatorios, y se sitúa entre la moral y el derecho.[21] Intenta, además de definir normas aplicables a situaciones concretas, definir lo que es conveniente, e incluso proporcionar guías de orientación para las conductas de las personas.[22] Está orientada al deber, se refleja en normas y códigos que se les exigen a los profesionales, conlleva actuaciones específicas, y es aprobada por un colectivo de profesionales.[23] Si se habla de deontología profesional, ésta es el estudio de los deberes que tiene cada profesión.

4.2. Los colegios profesionales

4.2.1. Qué son

Un colegio profesional es una corporación de derecho público. Eso significa que es una institución peculiar porque, debido a su naturaleza mixta, ejerce funciones público-privadas.[24] De los colegios profesionales proceden los códigos deontológicos, que los miembros del

[19] Schwartz, "The nature of the relationship between corporate codes of ethics and behaviour.", citado en Delgado-Alemany, Blanco-Gónzalez, and Revilla-Camacho, "Códigos deontológicos: El rol de los colegios profesionales y las profesiones reguladas," 231-32.

[20] Rodríguez Ruiz, *Ética profesional y deontología*, 142.; Jeremy Bentham and Amnon Goldworth, *Deontology ; Together with a Table of the Springs of Action ; and the Article on Utilitarianism* (Oxford: Clarendon Press, 1983).; Jeremy Bentham, *Deontología o Ciencia de la Moral*, 2 vols. (Valencia: Librería de Mallen y sobrinos, 1835).

[21] Delgado-Alemany, Blanco-Gónzalez, and Revilla-Camacho, "Códigos deontológicos: El rol de los colegios profesionales y las profesiones reguladas," 232.

[22] García Fernández, "Ética y deontología," 72.

[23] Helin and Sandström, "An inquiry into the study of corporate codes of ethics.", citado en Delgado-Alemany, Blanco-Gónzalez, and Revilla-Camacho, "Códigos deontológicos: El rol de los colegios profesionales y las profesiones reguladas," 232.

[24] "¿Qué son los colegios profesionales y para qué sirven? Conócelo en 5 puntos," (Unión Profesional, 2021), 3. https://unionprofesional.com/cuadernillos/.

colegio profesional, además de los profesionales a quienes van dirigidos, están obligados a cumplir.[25] Son instituciones reconocidas por la Constitución Española (art. 36), y no son ni asociaciones (art. 22), ni sindicatos (art. 28), ni asociaciones empresariales (art. 7), ni fundaciones (art. 34), ni organizaciones profesionales (art. 52), ni nada similar; son corporaciones de derecho público que tienen unas funciones muy específicas y necesarias como entidades de vertebración social. Sus objetivos esenciales son: ordenar el ejercicio de las profesiones, representar exclusivamente a las profesiones cuando estén sujetas a colegiación obligatoria, defender los intereses profesionales de los colegiados, y proteger los intereses de los consumidores y usuarios de los servicios de sus colegiados.

En España, los colegios profesionales se rigen por la Ley 2/1974. Las competencias sobre ordenación de colegios profesionales están transferidas a las comunidades autónomas, y esto quiere decir que cada comunidad autónoma puede autorizar la creación de sus propios colegios y desarrollar su propia normativa.[26] Para crear un colegio profesional, se necesita que la profesión esté regulada teniendo en cuenta, además, el artículo cuatro de la mencionada Ley 2/1974, cuyo título es "Creación, fusión, absorción, segregación, denominación y disolución de los Colegios Profesionales", destacando el apartado 3, que establece que "Dentro del ámbito territorial que venga señalado a cada Colegio no podrá constituirse otro de la misma profesión".

Los colegios profesionales fueron creados por los poderes públicos, para realizar un control independiente e imparcial de la actividad profesional, que permita a la ciudadanía ejercer sus derechos con garantías plenas.[27] Los colegios profesionales actualizan constantemente las normativas, las iniciativas y los proyectos que pueden afectar a la profesión, y al servicio que prestan a sus clientes y pacientes.[28] Además, ofrecen servicios diversos, como bolsa de empleo, asistencia jurídica, seguro de responsabilidad civil, biblioteca, etc.

---

[25] Delgado-Alemany, Blanco-Gónzalez, and Revilla-Camacho, "Códigos deontológicos: El rol de los colegios profesionales y las profesiones reguladas," 237.

[26] Delgado-Alemany, Blanco-Gónzalez, and Revilla-Camacho, "Códigos deontológicos: El rol de los colegios profesionales y las profesiones reguladas," 235.

[27] "¿Qué son los colegios profesionales y para qué sirven? Conócelo en 5 puntos," 8.

[28] "¿Qué son los colegios profesionales y para qué sirven? Conócelo en 5 puntos," 9.

4.2.2. Función deontológica

La función deontológica de los Colegios Profesionales es contemplada en el Artículo 36 de la Constitución Española, que establece que la Ley regulará las peculiaridades propias del régimen jurídico de los Colegios Profesionales, y el ejercicio de las profesiones titulares.[29]

Se basa, principalmente, en dos funciones: capacidad autorreguladora y potestad sancionadora.[30] La capacidad autorreguladora es la capacidad de los colegios profesionales de proclamar y aprobar las normas que rigen la profesión; estas normas deben ser cumplidas, obligatoriamente, por los profesionales colegiados, incluso por los que no lo son, ya que realizan actos propios de la profesión en particular. La potestad sancionadora está profundamente vinculada a la capacidad de aprobación del código deontológico, que debe cumplirse obligatoriamente, por lo que su incumplimiento implica que el ente que la promulgó tenga la capacidad de sancionar, desarrollando previamente un régimen de sanciones y faltas incorporado en los Estatutos y aprobándose legalmente por el Gobierno.[31] Sin embargo, conviene aclarar que, en España, hay dos tipos de profesiones: las reguladas por Ley, que tienen competencias profesionales exclusivas, y las que no están reguladas por Ley, que no tienen esas competencias.

Una profesión regulada por Ley es una profesión cuyo ejercicio debe cumplir varias normas y requisitos establecidos por una autoridad competente.[32] En la mayor parte de los casos, para poder ejercer las profesiones reguladas se necesita un título o certificado específico. Las profesiones reguladas suelen tener relación con actividades que requieren mucha competencia y responsabilidad, como la medicina, la ingeniería o la abogacía; esto es debido a que el ejercicio de esas profesiones puede conllevar tratar directamente con la vida y con el bienestar de las personas. En algunos países, hay muy pocas profesiones reguladas, no siendo el caso de España, país en el que hay muchas. Las áreas de las profesiones reguladas son la Sanidad y la

[29] Delgado-Alemany, Blanco-Gónzalez, and Revilla-Camacho, "Códigos deontológicos: El rol de los colegios profesionales y las profesiones reguladas," 236.

[30] Delgado-Alemany, Blanco-Gónzalez, and Revilla-Camacho, "Códigos deontológicos: El rol de los colegios profesionales y las profesiones reguladas," 236.

[31] Múzquiz Vicente-Arche, *La función deontológica de las organizaciones colegiales y su impacto económico y social*., citado en Delgado-Alemany, Blanco-Gónzalez, and Revilla-Camacho, "Códigos deontológicos: El rol de los colegios profesionales y las profesiones reguladas," 236.

[32] Infoeducación.es, "Listado de profesiones reguladas en España divididas por áreas." https://infoeducacion.es/profesiones-reguladas-espana/.

Salud, la de Ingeniería, la Social (abarca profesiones en las que se trabaja con otras personas), y la Jurídica. Además, hay profesiones reguladas fuera de estas áreas; por ejemplo, técnico/a superior en prevención de riesgos laborales, economista o físico/a.

Una vez hecha una explicación sobre los códigos deontológicos y sobre los colegios profesionales, conviene abordar el ámbito sobre el que se va a realizar este trabajo, que es la Gestión Digital de la Información y la Documentación. Para ello se explicará, en el siguiente apartado, en qué consiste el Grado en Gestión Digital de Información y Documentación de la Universidade da Coruña, y la situación de este grado en el resto de España, para proporcionarnos un contexto adecuado desde el que podamos reflexionar, después, sobre los códigos deontológicos existentes en este campo y sus posibilidades de desarrollo.

4.3. El Grado en Gestión Digital de Información y Documentación

4.3.1. En qué consiste. El caso de la Universidade da Coruña

El Grado en Gestión Digital de Información y Documentación, de la Universidade da Coruña, forma a profesionales con conocimientos multidisciplinares en *Information Science*, *Data Science*, *Big Data*, ciencias sociales, gestión de contenidos, comunicación y humanidades.[33] Tiene cinco perfiles profesionales: ingeniero/a de datos, productor/a de contenidos digitales, *community manager*, científico/a de datos y *business intelligence*. Tras finalizar el grado, las habilidades que se tendrán son las siguientes:

1. Dirigir equipos multidisciplinares que sean intermediarios entre la dirección de la empresa y los equipos de científicos e ingenieros de datos que gestionan y analizan la información.

2. Liderar el proceso de transformación digital de cualquier empresa, a través de las capacidades de gestión de contenidos y comunidades digitales.

3. Gestionar y planificar, de forma eficaz, los servicios de la información, que son los centros de documentación, los archivos y las bibliotecas.

[33] Facultade de Humanidades e Documentación, "Grado en Gestión Digital de Información y Documentación." https://humanidades.udc.es/estudos/gdid/informaci%C3%B3n-del-t%C3%ADtulo.

El perfil profesional de este grado tiene tanto formación humanística como formación técnica. El grado es único en Galicia, tiene una duración de cuatro cursos académicos y se imparte en la Facultad de Humanidades y Documentación de Ferrol.

4.3.2. Situación en España

En España, este grado también se imparte en Madrid, Barcelona y Murcia. En Madrid, se llama "Grado en Gestión de la Información y Contenidos Digitales"; se estudia en la Universidad Carlos III, en la Facultad de Humanidades, Comunicación y Documentación (campus de Getafe), y tiene una duración de cuatro años.[34] En Barcelona, se llama "Grado en Gestión de Información y Documentación Digital"; se estudia en la Universitat de Barcelona, y también dura cuatro cursos.[35] En Murcia, se denomina "Grado en Gestión de Información y Contenidos Digitales; se estudia en la Facultad de Comunicación y Documentación, y también tiene una duración de cuatro cursos.[36]

Tras explicar el Grado en Gestión Digital de Información y Documentación, tanto de la Universidade da Coruña como del resto de España, se tratará, en el siguiente apartado, el tema de los códigos deontológicos con más profundidad; concretamente, se indicará qué proceso hay que llevar a cabo para elaborar un código deontológico.

[34] Universidad Carlos III de Madrid, "Grado en Gestión de la Información y Contenidos Digitales." https://www.uc3m.es/grado/contenidos-digitales#programa.

[35] Universitat de Barcelona, "Grado en Gestión de Información y Documentación Digital." https://web.ub.edu/es/web/estudis/w/grado-G1098?subjects.

[36] Universidad de Murcia, "Grado en Gestión de Información y Contenidos Digitales." https://www.um.es/web/estudios/grados/contenidos-digitales.

4.4. Proceso para la elaboración de un código deontológico

El proceso para elaborar un código deontológico depende, en gran medida, de la organización, su historia, sus aspiraciones y su entorno. A continuación, se indican sus diferentes fases.[37]

4.4.1. Primera fase

En la primera fase, hay que hacer un análisis profundo de la realidad de la organización, o del campo profesional, y de su entorno. En primer lugar, se debe analizar la estructura de la organización y de la profesión mediante el estudio de los documentos legales y constitucionales, y los documentos públicos que contienen información relevante de la profesión. Además, es importante analizar la historia y la organización de la profesión.

En segundo lugar, hay que realizar un análisis de la cultura de la profesión, en la que se estudien los valores, costumbres, formas de actuar de los profesionales, y su visión. La aportación de los "informantes estratégicos" y de los órganos de gobierno profesional es fundamental para conocer la realidad de la cultura profesional, y para conocer la cultura organizativa que desean alcanzar y a la que aspiran.

En tercer lugar, se debe realizar un análisis del entorno-social. Consiste en analizar el entorno sociopolítico y normativo en el que actúa el/la profesional. Las normas sectoriales, la legalidad mercantil y las recomendaciones de organizaciones internacionales y asociaciones profesionales muy prestigiosas, afectan decisivamente a lo que es y puede llegar a ser la profesión. Además de esto, es muy importante conocer qué opinan y a qué aspiran los clientes y otros grupos de interés afectados por el ejercicio profesional.

En cuarto lugar, hay que hacer un análisis del entorno jurídico, político y social de la profesión. Consiste en analizar el marco legal y de organización política, además de los rasgos culturales esenciales del entorno social de la organización. Estos rasgos culturales nos deben indicar, más o menos, el nivel que tiene la conciencia moral de la sociedad en la que la organización está incluida.

[37] "Deontología Profesional. Los códigos deontológicos," (Unión Profesional, 2009), 18-20. https://unionprofesional.com/estudio/deontologia_profesional/.

4.4.2. Segunda fase

En la segunda fase, hay que redactar una primera propuesta para debatirla con profesionales prestigiosos y los órganos de gobierno del colectivo de profesionales. Esta propuesta tiene que presentar, de forma estructurada y lo más completa posible, la información que se recogió en la primera fase. Es importante que, en esta fase, participen personas de ámbitos profesionales diferentes, para que la redacción final contenga, por un lado, la manera en la que se sienten las personas implicadas en el gobierno de la profesión y, por otro lado, el sentir de las personas que ejecutan las tareas diarias. El código debe ser una herramienta útil para todos los profesionales.

4.4.3. Tercera fase

En la tercera fase, se realiza la redacción definitiva del código. Esta redacción debe ser hecha por miembros del colectivo profesional, apoyándose de una participación activa de los órganos de gobierno y de la ayuda de personas expertas en ética. En esta redacción, se debe realizar una síntesis de los rasgos fundamentales del carácter de la profesión, y de los compromisos que esta tenga en el futuro.

4.4.4. Fase transversal de sensibilización y formación

Además de las tres fases anteriores, es conveniente desarrollar una fase transversal de sensibilización y formación. El motivo de esto es que se necesita, claramente, un código ético comprensivo que pueda establecer expectativas de conducta, y que sirva para evaluar la toma de decisiones. Sin embargo, hay que llevar a cabo un entrenamiento para pensar éticamente.

Las pautas básicas de esta fase son la siguientes:

a. Los colegios profesionales deben evitar la dispersión, e ir a una ordenación de normas.

b. Las normas deontológicas deben ser normalizadas, y hay que modificar estatutos y reglamentos obsoletos.

c. Se deben introducir, además de buenos principios generales, casuística, que refleje la praxis profesional.

d. Se deben realizar revisiones continuas, para adecuar las normas a la realidad.

e. Las normas tienen que ser suficientemente publicitadas.

f. Hay que respetar correctamente el procedimiento sancionador.

4.5. Evoluciones en la deontología profesional

4.5.1. Formación continuada

La formación continuada debería ser una obligación esencial en cualquier profesional, como ya sucede en Europa, y el colegio profesional tendría que actuar positivamente para asegurar que se mantenga la capacitación profesional de sus miembros.[38] Si la corporación promueve la formación continuada de sus profesionales, se ayudará a garantizar que se cumplan los estándares de conducta en los que se basa.

La formación continuada de los trabajadores y de las trabajadoras tiene que ser incrementada por los colegios profesionales, porque es también una de sus competencias, y de las más importantes.[39] En cuanto al ámbito de la docencia, hay un casi total consenso en que el profesorado, su formación continuada o desarrollo, los aprendizajes y el ejercicio de la docencia son temas fundamentales en el sistema educativo de cualquier país.[40] Estos aspectos afectan a las personas que desempeñan su profesión, a los centros donde estas trabajan, a la educación del alumnado y a la sociedad. No obstante, hay controversias, desavenencias y preguntas que resolver sobre lo que hay en juego, la forma de afrontarlo y las posibles consecuencias.

Además de la formación continuada, existe otro aspecto fundamental dentro de la evolución de la deontología profesional: el respeto a la naturaleza y al medio ambiente. La razón principal de ello es que vivimos en un mundo en el que el cambio climático es una realidad, por lo que las diferentes profesiones deben involucrarse, en mayor o menor medida, para luchar contra

[38] "Deontología Profesional. Los códigos deontológicos," 28.

[39] Carmen Verde-Diego and Óscar Cebolla Bueno, "Deontología profesional: la ética denostada," *Cuadernos de trabajo social* 30, no. 1 (2017): 88.

[40] Juan M. Escudero Muñoz, "Un cambio de paradigma en la formación continuada del profesorado: escenario, significados, procesos y actores," (2020): 98.

este fenómeno. Para ello, resulta necesario que se creen códigos deontológicos que incluyan postulados ambientales, y este tema se desarrollará en el siguiente subapartado.

4.5.2. El respeto a la naturaleza y al medio ambiente

El respeto a la naturaleza y al medio ambiente es, indudablemente, un elemento que se debe tener en cuenta en el futuro, en todos los sectores de la sociedad, desde las empresas hasta los particulares, e incluyendo los profesionales liberales.[41] La Constitución hace referencia a este problema en el artículo 45, en el que indica que los poderes públicos velarán por el medio ambiente y que todo el mundo debe conservarlo. Una de las preocupaciones que deben tener los profesionales cuando ejercen su profesión, es la de respetar y conservar la naturaleza y el medio ambiente. Esa preocupación podrá incluirse en las respectivas normas deontológicas de la manera que la profesión estime conveniente, pero existe la posibilidad de enunciar, de forma general, directrices. Algunas de estas directrices son la no aceptación, por parte del profesional, de encargos o propuestas que son claramente perjudiciales para el medio ambiente, ya que constituye un deber ético que merece ser enunciado en la deontología profesional.

La ecoética (ética ambiental) es una ética aplicada del cuidado, que se puede materializar, más directamente y de forma más vinculante, mediante diversos postulados ambientales incluidos en los códigos deontológicos, de forma que se trate una perspectiva que abarque la consecución de los Objetivos de Desarrollo Sostenible, también en las profesiones más adecuadas para poner en práctica esos postulados, debido a que dañan mucho el medioambiente.[42] La ecoética, entonces, se presentaría no solamente como un imaginario colectivo y un cambio epistemológico de pensamiento en los aspectos productivos del sistema mundial, sino también como una guía sobre las acciones y conductas que se deben realizar, tanto en las profesiones más lesivas con el medioambiente, como en la sociedad en general. Los códigos deontológicos directamente ecoéticos prácticamente solo pueden existir en Veterinaria y en Ciencias Ambientales, y sin embargo no en muchas profesiones muy lesivas con el medioambiente.[43] Es necesario incluir, además de contenidos ecoéticos en las

[41] "Deontología Profesional. Los códigos deontológicos," 28-29.

[42] David Martín Sánchez, "La construcción de la ecoética en España y la proyección de futuro de su aplicación laboral mediante la deontología ambiental," *Observatorio medioambiental*, no. 25 (2022): 184.

[43] Martín Sánchez, "La construcción de la ecoética en España y la proyección de futuro de su aplicación laboral mediante la deontología ambiental," 192.

profesiones más lesivas con el medioambiente, códigos deontológicos que aseguren que los contenidos ecoéticos estudiados se apliquen, con posterioridad, en la práctica laboral de esas profesiones (ingeniería, arquitectura, química, etc.)

Los Colegios Oficiales son vitales para dar a la ecoética el protagonismo que debería tener en el ejercicio de algunas profesiones.[44] Es importante que se acompañe la creación de códigos deontológicos con la formación ecoética y ambiental, y con reformas drásticas en los currículums, sobre todo de las profesiones que tienen una función lesiva o extractiva con el medioambiente. Apenas existen códigos deontológicos ambientales, y aún menos trabajos de investigación sobre cómo incluir esos códigos, o sobre cómo conceptualizar, de forma adecuada, una deontología ambiental como tal.

Una de las mejores revistas internacionales de ética ambiental (*Environmental Ethics*), se empezó a publicar en 1979, y en Estados Unidos, Alemania, Gran Bretaña o algún país nórdico ya se debatía y publicaba, desde hace años, sobre ética ambiental.[45] En España, la ética ambiental, como disciplina sistemática, empezó su trayectoria en la segunda mitad de los años ochenta; no obstante, solo en algunos ámbitos y entre algunos intelectuales, no considerando la Academia filosófica su producción como un asunto relevante.

Arne Naess, filósofo sueco, acuñó el término "ecología profunda" para designar "un proceso de reflexión que conduzca a la acción", en respuesta a la necesidad de que el ser humano transforme la relación con su entorno.[46] Varias filosofías posmodernas se desarrollaron para combatir la crisis ambiental; pero lo que diferencia a la filosofía de Arne Naess de estas últimas es, quizás, su disposición a la acción, característica que propició que fuera muy criticada por sus detractores, aunque también logró reunir muchos seguidores.

---

[44] Martín Sánchez, "La construcción de la ecoética en España y la proyección de futuro de su aplicación laboral mediante la deontología ambiental," 196.

[45] María Carmen Velayos Castelo, "La ecoética en España," *La albolafia: revista de humanidades y cultura*, no. 2 (2014): 129-30.

[46] Pablo Corcuera and Leticia Ponce de León G, "Tendencias de los movimientos conservacionistas y el surgimiento de la Eco-Ética," *Sociológica México*, no. 56 (2015): 206.

4.5.3. Las Sociedades Profesionales como nuevos sujetos de la Deontología

Otra novedad, que debería aparecer en todos los códigos deontológicos, es la de las Sociedades Profesionales como nuevos sujetos de la Deontología.[47] La Deontología ahora es válida en otros campos de la organización profesional, además de en el ámbito corporativo. En este proceso de ampliación jugó un papel fundamental la aprobación de la Ley 2/2007 de sociedades profesionales, cuyo artículo 9 amplía a esas sociedades el ámbito de aplicación de las normas deontológicas corporativas. Esto significa que no solamente los profesionales colegiados se integran como sujetos de las normas éticas profesionales, sino que lo hacen también las sociedades que ellos mismos constituyan y que reúnan los caracteres definidos en la ley mencionada. El artículo 9 dice exactamente, en el apartado 1, que la sociedad profesional y los profesionales que actúan en su seno ejercerán la actividad profesional que constituya el objeto social de conformidad con el régimen deontológico y disciplinario propio de la correspondiente actividad profesional.[48]

Además de la formación continuada, las Sociedades Profesionales y el respeto a la naturaleza y al medio ambiente, existen otras evoluciones en la deontología profesional, de las que se hablará, brevemente, en el siguiente subapartado. Estas evoluciones son la precisión del contenido de determinados artículos, la mención de la función e interés general de la profesión, y la actualización de algún artículo debido a la aparición de las tecnologías de la información.

4.5.4. Otras evoluciones

Generalmente, es imprescindible la precisión del contenido de los artículos que pueden parecer ambiguos, o que no son contundentes a la hora de indicar las normas para que su obligado cumplimiento o vulneración no se interprete en ningún caso.[49]

También es conveniente moldear, quizás precediendo a los artículos, la función social y el interés general de la profesión. En España, la gran mayoría de los códigos deontológicos tienen

---

[47] "Deontología Profesional. Los códigos deontológicos," 29.

[48] Jefatura del Estado, "Ley 2/2007, de 15 de marzo, de sociedades profesionales," (2007). https://www.boe.es/buscar/act.php?id=BOE-A-2007-5584.

[49] "Deontología Profesional. Los códigos deontológicos," 29.

un preámbulo que expone lo importante y relevante que es una profesión, y/o que hace un histórico de códigos deontológicos anteriores.[50] Además, estos códigos deontológicos justifican la necesidad de su aprobación, o de su existencia, ampliación y adaptación si son más recientes.

Finalmente, es necesario actualizar alguno de los artículos a los nuevos usos profesionales que aparecen con el avance de las nuevas tecnologías de la comunicación.[51] Un ejemplo de estos nuevos usos profesionales es el ejercicio profesional "online" y a través de internet.

4.6. Los códigos deontológicos en el ámbito internacional

En el ámbito internacional, se elabora una gran cantidad de códigos deontológicos; esto sucede en cada país, en un área geográfica determinada para cada profesión, o con la finalidad de cubrir todas las profesiones.[52]

A medida que los códigos deontológicos abarcan más países, su contenido se vuelve más general, ya que cada país tiene características concretas que no se pueden contemplar. Esto sucede más cuando, además de muchos países diferentes, se intenta abarcar diferentes profesiones; en este caso, la generalización debe ser máxima, convirtiéndose en una enumeración de principios básicos en la mayor parte de los casos. Este carácter general no provoca que disminuya el valor de los códigos internacionales; sino que es necesario establecer unos elementos fundamentales comunes en un primer nivel, e ir desarrollándolos en los siguientes niveles, viendo las especificidades que existen en el ámbito nacional.

El Consejo Europeo de la Profesiones Liberales (CEPLIS), que es la asociación que representa a las profesiones liberales a nivel comunitario, elaboró los *Common values of the liberal professions in the European Union* (Valores comunes para las profesiones liberales en

[50] Delgado-Alemany, Blanco-Gónzalez, and Revilla-Camacho, "Códigos deontológicos: El rol de los colegios profesionales y las profesiones reguladas," 243.

[51] "Deontología Profesional. Los códigos deontológicos," 29.

[52] "Deontología Profesional. Los códigos deontológicos," 31.

la Unión Europea) que establecen los principios que deberían recoger los códigos de conducta del entorno de la Unión Europea.[53] Estos valores son: [54]

1. Confidencialidad
2. Formación continua
3. Independencia e imparcialidad
4. Conflictos de interés
5. Honestidad e integridad
6. Supervisión del personal de apoyo
7. Cumplimiento con los Códigos de Conducta y Práctica
8. Seguro de responsabilidad civil profesional
9. Conflicto con las creencias morales o religiosas
10. Informaciones relevantes a clientes y pacientes
11. Controversias
12. Asunción de responsabilidad
13. Actividades multidisciplinares
14. Habilidades lingüísticas
15. Comunicaciones
16. Formación en estándares éticos.
17. Buen Gobierno

5. Resultados

Una vez expuesto el marco de referencia se expondrán, en este apartado, los códigos deontológicos de cada uno de los tres países indicados anteriormente. La finalidad de esta acción es la de elaborar unas conclusiones en las que, por una parte, se aborden los objetivos del trabajo y, por otra parte, se exponga si la hipótesis planteada se cumple o no.

[53] "Deontología Profesional. Los códigos deontológicos," 32.

[54] Ceplis, "Los Valores Comunes de las Profesiones Liberales en la Unión Europea. Versión revisada-2014," (Bruselas, 2014), 2-7. https://ceplis.org/common-value/.

5.1. España

5.1.1. Principios fundamentales del derecho a la Protección de Datos [55]

1. Un principio fundamental del derecho a la Protección de Datos, es en el que se pone de manifiesto que los datos personales solamente podrán ser tratados de forma lícita, leal y transparente. Además, los datos deberán estar limitados a lo que se necesite en relación con motivos determinados, explícitos y legítimos.

2. Otro principio fundamental del derecho a la Protección de Datos es el de legitimación. Está directamente relacionado con el deber de la información, por el cual el titular de los datos debe ser informado, con absoluta claridad, sobre las finalidades para las que se recogen sus datos. El artículo 13 del Reglamento General de Protección de Datos incluye toda la información que se debe proporcionar a las personas interesadas cuando se recaban sus datos personales. El Big Data puede llevar a situaciones en las que el objetivo inicial para el que se recogió el dato quede, al menos, "difuminado" una vez el dato es explotado.

5.1.2. Código de Ética de un/una *Community Manager*

https://www.openinnova.es/codigo-de-etica-de-un-community-manager-es-fundamental/
(se visitó el 9 de agosto de 2023)

1. Tratar de manera justa y honesta con el público en general.

2. Evitar crear o publicar contenido, publicaciones o respuestas que contengan un énfasis innecesario en las características personales, incluidos el género, la raza, la etnia, la nacionalidad, la edad, la orientación sexual, las relaciones familiares, las creencias religiosas, o la discapacidad física o intelectual.

3. No participar nunca en un hostigamiento racial o de género para aumentar el tráfico o el compromiso.

[55] AEPD (http://www.agpd.es) and ISMS Forum (http://www.ismsforum.es), "Código de buenas prácticas en protección de datos para proyectos Big Data," (2017), 6. https://www.aepd.es/es/documento/guia-codigo-de-buenas-practicas-proyectos-de-big-data.pdf.

4. Hacer todo lo posible, dentro de las capacidades profesionales, para garantizar la conducta razonable de los miembros dentro de sus comunidades. Se debe informar de cualquier forma de hostigamiento, tanto dirigida a ellos como a otras personas, a su empleador o a las plataformas en las que se realiza esta actividad.

5. Hacer todo lo posible para mantenerse al día con toda la legislación relevante en sus regiones de práctica y ubicaciones comunitarias, que se debe cumplir en todo momento. Nota: esto no impide abogar por el cambio de esta regulación o informar de su evolución.

6. Cumplir con todas las reglas y términos relevantes en las plataformas en las que operan. El cumplimiento no impide que los *Community Managers* ofrezcan críticas constructivas a las plataformas, o que presenten quejas formales si es necesario.

7. Respetar las regulaciones de copyright. Los *Community Managers* deben solicitar permiso para volver a publicar contenido de otras fuentes, y deben atribuir correctamente todo el contenido protegido por derechos de autor al propietario original o licenciatario (en el caso de *Creative Commons* o similar).

8. Revelar cualquier conflicto de interés personal, y no permitir que los pagos, obsequios o beneficios socaven la precisión o imparcialidad de sus interacciones con los empleadores, sus comunidades y el público en general. Evitar conductas o prácticas que puedan desacreditar a los mismos.

9. No divulgar, deliberadamente, información falsa o engañosa, y tener cuidado de corregir los errores y emitir correcciones tan pronto como sea posible. Cuando se verifique que los miembros de la comunidad hayan publicado información privada de otra persona, los *Community Managers* falsos o difamatorios actuarán para eliminarla de manera oportuna.

5.1.3. Los principios de la ética de los datos

https://nuestrosdatosseguros.es/los-principios-de-la-etica-de-los-datos/#:~:text=5%20principios%20de%20la%20%C3%A9tica%20de%20los%20datos
(se visitó el 9 de agosto de 2023)

La ética de los datos es la rama que evalúa las prácticas de recopilación, análisis y tratamiento del *Big Data* que pueden afectar a las personas y a la sociedad.

1. Propiedad: las empresas y las organizaciones deben saber que los usuarios son los dueños de los datos.

2. Transparencia

Las empresas y las organizaciones deben ser transparentes en cuanto al tipo de datos que recopilan y almacenan, en cuanto a la finalidad de esa recopilación y almacenamiento, y en cuanto para qué utilizarán esos datos. Ejercer la transparencia permite que se corrijan prácticas discriminatorias, sobre todo en la recolección de datos; por ejemplo, si una empresa explica con qué criterios entrena sus algoritmos, es más fácil que puedan detectarse datos sesgados o malinterpretados que excluyan a una determinada parte de la población. Actualmente, y aunque a veces sea más por motivos de reputación corporativa que por motivos éticos, la realidad es que son muchas las empresas que se están sumando a la causa de la transparencia y la integridad, ya que, en última instancia, es cada vez más importante para ganarse la confianza y la fidelidad de los usuarios y consumidores. Y es que, en la era digital, la confianza en una organización también se mide por la forma que tienen de gestionar los datos. Para saber si una empresa está utilizando de manera ética y transparente el *Big Data* debe preguntarse a sí misma si contaría sin problemas a sus clientes cómo utiliza dichos datos.

3. Protección y privacidad de los datos

Las empresas y organizaciones que gestionan datos deben garantizar la seguridad y la privacidad de los datos. A veces, estos conceptos se confunden entre sí o se utilizan como sinónimos cuando realmente no son solo distintos, sino que también complementarios. Además, ambos son esenciales para poder hablar de seguridad de los datos. Es decir, diremos que los datos serán seguros en la medida que cumplan las exigencias de seguridad y privacidad. Por seguridad de los datos (del inglés, *data security*) se entiende todo lo que hace referencia a la protección de los datos contra accesos no autorizados, y es un concepto que tiene que ver con aspectos técnicos, ya que de lo que se trata es de evitar por medios tecnológicos que terceros no deseados se hagan con los datos. Por privacidad (del inglés, *data privacy*), en cambio, nos referimos a la protección de la identidad y en este caso hace referencia al acceso autorizado a los datos, es decir, quién lo tiene, quién lo define y para qué finalidad, y no se trata pues de una cuestión técnica sino más bien legal.

4. Propósito e intencionalidad

¿Qué van a hacer con nuestros datos? En ética, los propósitos o intenciones son importantes. Así, si el objetivo de la recopilación de datos es beneficiarse de las debilidades de los usuarios, vender información personal o cualquier otra intención maliciosa, se están traspasando los límites éticos.

Incluso cuando las intenciones son buenas, empresas y organizaciones deben preguntarse sobre la necesidad o no de solicitar y recopilar cada dato, sobre todo los más personales.

Un ejemplo: en un estudio sobre el riesgo de reincidencia delictiva de presos se tienen en cuenta datos como la raza o el sexo. Aunque los datos se piden por una buena causa, no es ético recopilar esos datos, ya que pueden contribuir a un análisis final parcial y sesgado. La idea es, pues, extraer el mínimo de información y datos personales necesarios para dicho estudio.

Otro ejemplo de uso poco ético de los datos es el *Social Credit System* de China, que basándose en el conocimiento exhaustivo de todo lo que hacen sus ciudadanos, también en su vida privada, genera un sistema de clasificación de los individuos que condiciona aspectos tan importantes como las oportunidades de empleo, el acceso a la vivienda o la concesión de un crédito.

5. Sostenibilidad

Cuando una empresa u organización tiene en consideración los anteriores cuatro principios éticos y los integra en su estrategia corporativa global, hablamos de sostenibilidad ética. Y es que únicamente integrando la ética en lo más profundo de la cultura corporativa es posible garantizar que el respeto por los datos perdura en el tiempo. En este sentido resulta interesante el libro "*Data Ethics – The Rise of Morality in Technology*" de Jamie Bernard, considerado una guía exhaustiva acerca de cómo incorporar de manera efectiva y transversal la ética de los datos en las organizaciones.

5.2. Reino Unido

5.2.1. Guía para la Ciencia de Datos Ética

https://rss.org.uk/RSS/media/News-and-publications/Publications/Reports%20and%20guides/A-Guide-for-Ethical-Data-Science-Final-Oct-2019.pdf (se visitó el 4 de agosto de 2023)

Existen cinco temas éticos relevantes asociados a la ciencia de datos. Se trata de un resumen, y no pretende ser una lista exhaustiva de principios éticos. Los cinco temas a considerar son:

1. Tratar de aumentar el valor de la ciencia de datos para la sociedad

Dado que el impacto que la ciencia de datos puede tener en la sociedad podría ser significativo, una consideración ética importante es cuáles podrían ser las implicaciones potenciales para la sociedad en su conjunto. Un tema común en los marcos éticos de la ciencia de datos y la IA es que los profesionales intenten obtener resultados en su trabajo que contribuyan a mejorar el bienestar público. Esto podría implicar que los profesionales traten de compartir los beneficios de la ciencia de datos y equilibrarlo con el bienestar de las personas potencialmente afectadas.

2. Evitar daños

La ciencia de datos puede causar daños, por lo que esta consideración ética se centra en cómo los profesionales pueden evitarlo trabajando de forma que se respete la privacidad, la igualdad y la autonomía de las personas y los grupos, y denunciando los posibles daños o violaciones éticas. Los profesionales pueden estar sujetos a obligaciones legales y reglamentarias en relación con la privacidad de las personas, según la jurisdicción en la que trabajen, así como a la obligación reglamentaria de denunciar daños o violaciones de los requisitos legales. Esto también puede aplicarse al trabajo relacionado con empresas, animales o el medio ambiente, teniendo en cuenta los derechos comerciales, el bienestar de los animales y la protección de los recursos medioambientales.

3. Aplicar y mantener la competencia profesional

Este principio ético espera que los profesionales de la ciencia de datos apliquen las mejores prácticas y cumplan todos los requisitos legales y reglamentarios pertinentes, así como los códigos de los organismos profesionales aplicables. La competencia profesional implica la plena comprensión de las fuentes de error y sesgo en los datos, utilizando datos "limpios" (por ejemplo, editados para detectar valores ausentes, incoherentes o erróneos), y respaldar el trabajo con métodos estadísticos y algorítmicos sólidos que sean adecuados para la pregunta planteada. Los profesionales también pueden evaluar y sopesar a fondo los beneficios del trabajo frente a los riesgos que plantea, y revisar periódicamente los modelos.

4. Tratar de preservar o aumentar la fiabilidad

La confianza del público en el trabajo de los científicos de datos puede verse afectada por la forma en que se aplican los principios éticos. Los profesionales pueden contribuir a aumentar la fiabilidad de su trabajo teniendo en cuenta los principios éticos en todas las fases de un proyecto. Este es otro tema recurrente que anima a los profesionales a ser transparentes y honestos a la hora de comunicar cómo se utilizan los datos. La transparencia puede incluir la explicación completa de cómo se utilizan los algoritmos, si se ha delegado alguna decisión y por qué, y ser abiertos sobre los riesgos y sesgos. La participación de un amplio abanico de partes interesadas y la consideración de las percepciones del público, tanto desde el principio como a lo largo de los proyectos, puede ayudar a generar confianza y garantizar que se entienden todos los posibles sesgos potenciales.

5. Mantener la responsabilidad y la supervisión

Otra cuestión clave en la ética de los datos, en torno a la automatización y la IA, es cómo los profesionales mantienen la responsabilidad y la supervisión humanas en su trabajo. La rendición de cuentas puede incluir ser consciente de cómo y cuándo delegar la toma de decisiones en los sistemas, y disponer de una gobernanza que garantice que los sistemas cumplen los objetivos previstos. Cuando se decida delegar la toma de decisiones, sería útil comprender y explicar plenamente las posibles implicaciones de hacerlo, ya que el trabajo podría llevar a introducir sistemas avanzados de IA que no cuenten con una gobernanza adecuada. Los profesionales deben tener en cuenta que delegar cualquier decisión en estos sistemas no elimina ninguna de sus responsabilidades individuales.

5.2.2. Marco ético de los datos

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/923108/Data_Ethics_Framework_2020.pdf (se visitó el 4 de agosto de 2023)

Esta guía está dirigida a todos los que trabajan directa o indirectamente con datos en el sector público, incluidos los profesionales de los datos (estadísticos, analistas y científicos de datos), los responsables políticos, el personal operativo y los que ayudan a producir información basada en datos.

Principios generales

Los principios generales son aplicables a lo largo de todo el proceso y sustentan todas las acciones y todos los aspectos del proyecto.

1. Transparencia

La transparencia significa que sus acciones, procesos y datos están abiertos a una inspección mediante la publicación de información sobre el proyecto en un formato completo, abierto, comprensible, fácilmente accesible y libre. En su trabajo con y sobre datos y la IA, utilice las orientaciones disponibles, por ejemplo, el *Open Government Playbook*, para garantizar la transparencia en todo el proceso.

2. Rendición de cuentas

La rendición de cuentas significa que existen mecanismos eficaces de gobernanza y supervisión de cualquier proyecto. La rendición de cuentas pública significa que el público o sus representantes pueden ejercer una supervisión y un control efectivos sobre las decisiones y medidas adoptadas por el gobierno y sus funcionarios, a fin de garantizar que las iniciativas gubernamentales cumplen sus objetivos declarados y responden a las necesidades de las comunidades a las que van dirigidas.

3. Imparcialidad

Es crucial eliminar la posibilidad de que su proyecto tenga efectos discriminatorios involuntarios sobre individuos y grupos sociales. Debe tratar de mitigar los prejuicios que puedan influir en el resultado de su modelo y garantizar que el proyecto y sus resultados

respeten la dignidad de las personas, sean justos, no discriminatorios y coherentes con el interés público, incluidos los derechos humanos y los valores democráticos.

Acciones específicas

Acciones específicas le guiarán a través de las diferentes etapas del proyecto y le proporcionarán consideraciones prácticas.

1. Definir y comprender el beneficio público y la necesidad del usuario

Cuando se inicia un proyecto de datos del sector público, hay que articular claramente su finalidad. Esto incluye tener claro qué beneficio público pretende conseguir el proyecto y cuáles son las necesidades de las personas que utilizarán el servicio o se verán más directamente afectadas por él.

- Comprender el beneficio público más amplio.
- Comprender las consecuencias imprevistas o negativas de su proyecto.
- Consideraciones sobre derechos humanos.
- Justifique el beneficio para los contribuyentes y el uso adecuado de los recursos públicos en su proyecto.
- Hacer transparentes las necesidades de los usuarios y los beneficios públicos.
- Comprender las necesidades del usuario.
- Asegúrese de que el problema está claramente articulado antes de iniciar el proyecto.
- Compruebe si todos los miembros de su equipo entienden la necesidad del usuario y cómo puede ayudarle el uso de los datos.
- Repase una y otra vez las necesidades del usuario a lo largo del proyecto.

2. Cumplir la ley

Debe conocer las leyes y códigos de buenas prácticas relacionados con el uso de datos. En caso de duda, consulte a los expertos pertinentes.

- Obtenga asesoramiento jurídico.
- Es su deber y obligación cumplir la ley en cualquier proyecto de datos. Si está utilizando datos personales, debe cumplir con los principios del Reglamento General de Protección de Datos de la UE (GDPR) y la Ley de Protección de Datos de 2018 (DPA 2018),

que implementa aspectos del GDPR y transpone la Directiva de Aplicación de la Ley a la legislación del Reino Unido. También establece regímenes de tratamiento independientes para las actividades que quedan fuera del ámbito de aplicación de la legislación de la UE.

▪ La protección de datos desde el diseño y por defecto es un requisito legal en virtud del RGPD (véase el artículo 25). En virtud del artículo 35 del GDPR, es obligatorio realizar una evaluación del impacto sobre la protección de datos (DPIA) (también conocida como evaluación del impacto sobre la privacidad) cuando sea probable que exista un riesgo elevado para los derechos de las personas, en particular cuando se utilicen nuevas tecnologías. Es una buena práctica realizar una DPIA para cualquier uso de datos personales.

▪ Un aspecto importante del cumplimiento de la legislación sobre protección de datos es poder demostrar qué medidas se están tomando para garantizar que todo está documentado, como se indica en el artículo 5, apartado 2, del GDPR (principio de responsabilidad) y en el artículo 30 sobre el mantenimiento de registros de las actividades de tratamiento. Su organización y los equipos de garantía de la información serán responsables de esto a un alto nivel, incluida la garantía de que las políticas y la formación están en su lugar. Sin embargo, es esencial mostrar cómo se está haciendo esto a nivel individual, a través de la documentación exhaustiva de cosas como las Evaluaciones de Impacto de la Protección de Datos.

▪ Publique su DPIA y otros documentos relacionados.

▪ Garantice que el proyecto cumple la Ley de Igualdad de 2010.

▪ Garantice una gestión eficaz de sus datos.

▪ Garantice la conformidad de su proyecto con cualquier normativa adicional.

3. <u>Revisar la calidad y las limitaciones de los datos</u>

La calidad de las nuevas tecnologías depende de los datos y las prácticas utilizadas para crearlas. Debe asegurarse de que los datos del proyecto son precisos, representativos, proporcionales, de buena calidad y capaces de explicar sus limitaciones.

▪ Debe utilizar los datos mínimos necesarios para lograr el resultado deseado (artículo 5, apartado 1, letra c), del GDPR). Los datos personales deben ser adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que se tratan.

▪ Si tiene previsto anonimizar o seudonimizar datos personales antes de vincularlos o analizarlos, asegúrese de seguir el *ICO's Anonymisation*: código de prácticas de la gestión del riesgo para la protección de datos, y documente sus métodos.

▪ Si los datos no son sensibles ni personales, y si los Acuerdos de Intercambio de Datos con el proveedor lo permiten, debe hacer que los datos sean abiertos y asignarles un identificador de objeto digital (DOI). También puede publicar datos en *Find open data* y *UK Data Archive*.

5.2.3. La ética del Big Data

https://blog.hurree.co/the-ethics-of-big-data#:~:text=The%20field%20of%20big%20data%20ethics%20itself%20is%20defined%20as,of%20conduct%20for%20data%20use (se visitó el 7 de agosto de 2023)

El campo de la ética del Big Data se define como la definición, defensa y recomendación de conceptos de prácticas correctas e incorrectas en relación con el uso de datos, con especial énfasis en los datos personales. La ética del Big Data pretende crear un código de conducta ética y moral para el uso de los datos.

Hay cinco áreas principales de preocupación en la ética del Big Data que perfilan el potencial de uso inmoral de los datos:

1. Consentimiento informado

Consentir significa dar permiso sin coacción para que te ocurra algo.

El consentimiento informado es la forma más cuidadosa, respetuosa y ética de consentimiento. Requiere que el recopilador de datos haga un esfuerzo significativo para dar a los participantes una comprensión razonable y precisa de cómo se utilizarán sus datos.

En el pasado, el consentimiento informado para la recopilación de datos se tomaba normalmente para la participación en un único estudio. Los macrodatos hacen imposible esta forma de consentimiento, ya que el objetivo de los estudios, la minería y el análisis de macrodatos es revelar patrones y tendencias entre puntos de datos que antes eran inconcebibles. De este modo, no es posible que el consentimiento sea "informado", ya que ni el recopilador de datos ni el participante en el estudio pueden saber o comprender razonablemente qué se obtendrá de los datos o cómo se utilizarán.

Se han introducido revisiones en la norma del consentimiento informado. La primera se conoce como "consentimiento amplio", que autoriza previamente los usos secundarios de los

datos. La segunda es el "consentimiento escalonado", que autoriza usos secundarios específicos de los datos, por ejemplo, para la investigación del cáncer, pero no para la investigación genómica. Algunos argumentan que estas nuevas formas de consentimiento diluyen el concepto y dejan a los usuarios expuestos a prácticas poco éticas.

Otros problemas surgen cuando los interesados potencialmente "involuntarios" o desinformados obtienen su información de las plataformas de las redes sociales. Los contratos de servicios de las redes sociales suelen incluir el derecho a recopilar, agregar y analizar esos datos. Sin embargo, Ofcom descubrió que el 65% de los usuarios de Internet suelen aceptar los términos y condiciones sin leerlos. Por tanto, no es descabellado suponer que muchos usuarios finales no comprendan todo el alcance del uso de datos, que cada vez va más allá de la publicidad digital y se extiende a la investigación en ciencias sociales.

2. Privacidad

La ética de la privacidad implica muchos conceptos diferentes, como libertad, autonomía, seguridad y, en un sentido más moderno, protección y exposición de datos.

Se puede entender el concepto de privacidad del Big Data desglosándolo en tres categorías:

- La condición de la privacidad
- El derecho a la privacidad
- La pérdida de privacidad y la invasión

La escala y la velocidad del Big Data plantean una grave preocupación, ya que muchos procesos tradicionales de privacidad no pueden proteger los datos sensibles, lo que ha provocado un aumento exponencial de la ciberdelincuencia y las filtraciones de datos.

Un ejemplo de fuga de datos significativa que causó una pérdida de privacidad a más de 200 millones de usuarios de Internet ocurrió en enero de 2021. Un sitio de redes sociales chino en auge llamado “Sociallarks” sufrió una brecha debido a una serie de errores de protección de datos que incluían una base de datos ElasticSearch no segura. Un pirata informático pudo acceder a la base de datos que almacenaba:

- Nombres
- Números de teléfono
- Direcciones de correo electrónico
- Descripciones de perfiles
- Seguidores y datos de participación
- Ubicaciones
- Enlaces a perfiles de LinkedIn

▪ Nombres de acceso a cuentas de redes sociales conectadas

Otro motivo de preocupación es el creciente poder analítico de los macrodatos, es decir, cómo puede afectar a la privacidad cuando la información personal de varias plataformas digitales puede ser extraída para crear una imagen completa de una persona sin su consentimiento explícito. Por ejemplo, si alguien solicita un empleo, se puede obtener información sobre él a través de su huella digital para identificar sus inclinaciones políticas, su orientación sexual, su vida social, etc. Todos estos datos podrían utilizarse como motivo para rechazar una solicitud de empleo aunque la información no haya sido ofrecida voluntariamente por el solicitante.

3. Propiedad

Cuando hablamos de propiedad en términos de Big Data, nos alejamos de la comprensión tradicional o legal de la palabra como el derecho exclusivo a usar, poseer y disponer de una propiedad. En este contexto, la propiedad se refiere más bien a la redistribución de datos, la modificación de datos y la capacidad de beneficiarse de las innovaciones de datos.

En el pasado, los legisladores han dictaminado que, como los datos no son una propiedad ni una mercancía, no pueden ser robados; esta creencia ofrece poca protección o compensación a los usuarios de Internet y a los consumidores que proporcionan información valiosa a las empresas sin beneficio personal.

Podemos dividir la propiedad de los datos en dos categorías:

▪ El derecho a controlar los datos: editarlos, gestionarlos, compartirlos y eliminarlos.

▪ El derecho a beneficiarse de los datos: obtener beneficios del uso o venta de los datos.

En contra de la creencia común, quienes generan los datos, por ejemplo, los usuarios de Facebook, no son automáticamente propietarios de los mismos. Algunos incluso sostienen que los datos que proporcionamos para utilizar plataformas en línea "gratuitas" son en realidad un pago por esa plataforma. Pero los grandes datos son mucho dinero en el mundo actual. Muchos internautas creen que la balanza se inclina en su contra en lo que respecta a la propiedad de los datos y la transparencia de las empresas que los utilizan y se benefician de ellos.

En los últimos años ha cobrado fuerza la idea de monetizar los datos personales; la ideología pretende devolver la propiedad de los datos al usuario y equilibrar el mercado permitiendo a los usuarios vender sus datos legalmente. Se trata de un ámbito legislativo muy polémico, y algunos sostienen que designar los datos como mercancía es perder nuestra autonomía y libertades.

4. Sesgo y objetividad de los algoritmos

Los algoritmos son diseñados por humanos, los conjuntos de datos que estudian son seleccionados y preparados por humanos, y los humanos tienen prejuicios.

Hasta ahora, hay pruebas significativas que sugieren que los prejuicios humanos están infectando la tecnología y los algoritmos, e impactando negativamente en las vidas y libertades de los humanos. Especialmente los que pertenecen a las minorías de nuestras sociedades.

El llamado "sesgo codificado" se ha identificado en casos tan sonados como el descubrimiento por parte de Joy Buolamwini, investigadora del laboratorio del MIT, de un sesgo de tipo racial en los sistemas comerciales de inteligencia artificial creados por grandes empresas estadounidenses. Buolamwini descubrió que el software había sido entrenado en conjuntos de datos con un 77% de imágenes masculinas y más de un 83% de imágenes de piel blanca. Estos conjuntos de datos sesgados crearon una situación en la que el programa no reconoce los rostros masculinos blancos con una tasa de error de sólo el 0,8%, mientras que los rostros femeninos de piel oscura se detectan con una tasa de error del 20% en un caso y del 34% en los otros dos. Estos sesgos van más allá de las líneas raciales y de género y se extienden a las cuestiones de la elaboración de perfiles delictivos, la pobreza y la vivienda.

Los sesgos de los algoritmos se han convertido en una parte tan arraigada de la vida cotidiana que también se ha documentado que afectan a nuestra psique personal y a nuestros procesos de pensamiento. El fenómeno se produce cuando percibimos nuestra realidad como un reflejo de lo que vemos en Internet. Sin embargo, lo que vemos es a menudo una realidad a medida creada por algoritmos y personalizada a partir de nuestros hábitos previos de visionado. El algoritmo nos muestra contenidos que probablemente nos gusten o con los que estemos de acuerdo y descarta el resto. Cuando existen burbujas de filtros como esta, se crean cámaras de eco y, en casos extremos, pueden conducir a la radicalización, el sectarismo y el aislamiento social.

5. La brecha del Big Data

La brecha del Big Data trata de definir el estado actual del acceso a los datos. La comprensión y las capacidades de extracción de los macrodatos están aisladas en manos de unas pocas grandes empresas. Esta división crea "los que tienen" y "los que no tienen" Big Data y excluye a quienes carecen de los recursos financieros, educativos y tecnológicos necesarios para acceder a los grandes conjuntos de datos y analizarlos.

Tim Berners-Lee ha afirmado que la brecha del Big Data separa a las personas de datos que podrían ser muy valiosos para su bienestar. Y a pesar de la creciente industria de aplicaciones

que utilizan datos para mejorar nuestras vidas en términos de salud, finanzas, etc., actualmente no hay forma de que los individuos extraigan sus propios datos o conecten silos de datos potenciales que el software comercial pasa por alto. Una vez más, nos enfrentamos al problema ético de quién es el propietario de los datos que generamos; si nuestros datos no son nuestros para modificarlos, analizarlos y beneficiarnos de ellos en nuestros propios términos, entonces efectivamente no nos pertenecen.

La división de los datos crea más problemas cuando consideramos los sesgos de los algoritmos que clasifican a los individuos en categorías basadas en una culminación de datos a los que los propios individuos no pueden acceder. Por ejemplo, los programas informáticos de elaboración de perfiles pueden marcar a una persona como de alto riesgo potencial de cometer actividades delictivas, haciendo que las autoridades la detengan y la registren legalmente o incluso que se le deniegue la vivienda en determinadas zonas. La brecha del Big Data significa que los "pobres de los datos" no pueden entender los datos o métodos utilizados para tomar estas decisiones sobre ellos y sus vidas.

5.2.4. Ley de protección de datos de 2018

https://www.legislation.gov.uk/ukpga/2018/12/part/4/chapter/2/crossheading/the-data-protection-principles/enacted (se visitó el 23 de agosto de 2023)

Primer principio de protección de datos

(1) El primer principio de protección de datos es que el tratamiento de datos personales debe ser

(a) lícito, y

(b) leal y transparente.

(2) El tratamiento de datos personales sólo es lícito si y en la medida en que

(a) se cumpla al menos una de las condiciones del Anexo 9, y

(b) en caso de tratamiento sensible, se cumpla también al menos una de las condiciones del Anexo 10.

(3) El Secretario de Estado podrá modificar reglamentariamente el anexo 10

(a) añadiendo condiciones;

(b) omitiendo las condiciones añadidas mediante reglamentos en virtud del apartado (a).

(4) Los reglamentos en virtud del apartado (3) están sujetos al procedimiento de resolución afirmativa.

(5) Para determinar si el tratamiento de datos personales es leal y transparente, se tendrá en cuenta el método por el que se obtienen.

(6) A efectos del apartado (5), los datos se considerarán obtenidos de forma leal y transparente si consisten en información obtenida de una persona que

(a) esté autorizada por ley a suministrarla, o

(b) esté obligada a suministrarla en virtud de una ley o de una obligación internacional del Reino Unido.

(7) En el presente artículo, por "tratamiento sensible" se entenderá

(a) el tratamiento de datos personales que revelen el origen racial o étnico, las opiniones políticas, las convicciones religiosas o filosóficas o la afiliación sindical;

(b) el tratamiento de datos genéticos con el fin de identificar de manera inequívoca a una persona;

(c) el tratamiento de datos biométricos con el fin de identificar de manera unívoca a una persona;

(d) el tratamiento de datos relativos a la salud;

(e) el tratamiento de datos relativos a la vida sexual o a la orientación sexual de una persona;

(f) el tratamiento de datos personales relativos a

(i) la comisión o presunta comisión de un delito por una persona, o

(ii) un procedimiento por un delito cometido o presuntamente cometido por una persona, la resolución de dicho procedimiento o la sentencia de un tribunal en dicho procedimiento.

Segundo principio de protección de datos

(1) El segundo principio de protección de datos es que

(a) la finalidad para la que se recogen los datos personales, en cualquier ocasión, debe ser específica, explícita y legítima, y

(b) los datos personales así recogidos no deben tratarse de manera incompatible con la finalidad para la que se recogen.

(2) El apartado (b) del segundo principio de protección de datos está sujeto a los apartados (3) y (4).

(3) Los datos personales recogidos por un responsable del tratamiento, para un fin determinado, podrán tratarse para cualquier otro fin del responsable del tratamiento que haya recogido los datos, o para cualquier otro fin de otro responsable del tratamiento, siempre que

(a) el responsable del tratamiento esté autorizado por ley a tratar los datos para ese fin, y

(b) el tratamiento sea necesario y proporcionado a ese otro fin.

(4) El tratamiento de datos personales se considerará compatible con la finalidad para la que se recaben, si dicho tratamiento

(a) consiste en

(i)tratamiento con fines de archivo en interés público

(ii)tratamiento con fines de investigación científica o histórica, o

(iii) tratamiento con fines estadísticos, y

(b) está sujeto a las garantías apropiadas para los derechos y libertades del interesado.

Tercer principio de protección de datos

El tercer principio de protección de datos establece que los datos personales deben ser adecuados, pertinentes y no excesivos en relación con los fines para los que se traten.

Cuarto principio de protección de datos

El cuarto principio de protección de datos establece que los datos personales objeto de tratamiento deben ser exactos y, en caso necesario, actualizados.

Quinto principio de protección de datos

El quinto principio de protección de datos establece que los datos personales no deben conservarse más tiempo del necesario para los fines para los que se tratan.

Sexto principio de protección de datos

(1) El sexto principio de protección de datos establece que los datos personales deben tratarse de una manera que incluya la adopción de medidas de seguridad adecuadas, en relación con los riesgos derivados del tratamiento de datos personales.

(2) Los riesgos a los que se refiere el apartado (1) incluyen (pero no se limitan a) el acceso accidental, o no autorizado, a los datos personales, o su destrucción, pérdida, uso, modificación o divulgación.

5.3. Estados Unidos

5.3.1. Código ético para analistas de datos

https://www.blastanalytics.com/blog/code-of-ethics-for-data-analysts-8-guidelines (se visitó el 9 de agosto de 2023)

1. Proteja a sus clientes

Sus clientes suelen entregarle muchos datos personales. La PII (información personal identificable) debe protegerse rigurosamente. Lo último que desea es que su empresa aparezca en las noticias de la noche por una filtración de datos o un uso indebido de los mismos. Como regla general, pregúntele a un amigo que no pertenezca al sector: ¿me gustaría que se hicieran públicos estos datos sobre mí? Si la respuesta es "no", proceda en consecuencia.

2. Sea el portador de las malas noticias

No tenga miedo de ser el portador de las malas noticias. Es fácil dejarse llevar por el deseo de mostrar un progreso o crecimiento continuos, incluso cuando no existe ninguno. Usted no es sus números. Un trimestre negativo no es un reflejo de usted personalmente. Si los datos reflejan malas noticias, dígales por qué.

3. No fuerce los datos

Utilizar los datos de forma descuidada o intencionadamente errónea no es profesional. Cualquiera con una pizca de conocimientos de Excel puede hacer que un gráfico parezca mejor de lo que debería. Es fácil crear una tendencia fantasma o exagerar un pequeño repunte en las cifras. No lo haga. También hay que tener en cuenta que es fundamental ser dueño de los datos. Conozca los datos al dedillo para no mentir involuntariamente dando información errónea.

4. No haga favoritismos

Por mucho que nos gustaría tener siempre esa pepita de oro en nuestros análisis, a veces simplemente no la tenemos. No fabrique o adorne un punto que realmente pertenece al apéndice de su PowerPoint.

5. No mienta

Parece una obviedad. Sin embargo, he visto a muchos analistas mentir durante una presentación. El sello distintivo de cualquier gran analista es la confianza. Si sus cifras son erróneas, si hay un error tipográfico, reconózcalo. Corrija los errores. La confianza pagará dividendos a largo plazo. Sus colegas recordarán su integridad mucho después de que hayan olvidado que se equivocó de número en la diapositiva 12.

6. Comprenda el papel de la calidad de los datos

Nuestra directora de Estrategia Analítica, Aimee Bos, me ha recordado que la calidad de los datos es un tema muy importante. Comunicar datos erróneos como verdad es peor que no comunicar ningún dato. No crea ciegamente lo que le dice su herramienta de análisis. Entienda los fundamentos de lo que entra en esos números.

7. ¿Estoy mejorando el negocio?

Se pregunta: "¿Estoy mejorando el negocio, así como a nuestros clientes?". El valor para el cliente final y nuestro negocio debe estar siempre presente en nuestro pensamiento. Haga que sea la norma, no la excepción, que los clientes sean los dueños de sus datos y que estén seguros en sus manos.

8. La gobernanza de los datos es fundamental

Hablando con la veterana analista de Blast, Halee Kotara, hablamos de las múltiples veces que la gobernanza de datos ha desempeñado un papel en nuestro trabajo. Estamos de acuerdo en que es necesario poner orden y democratizar los datos. Sin embargo, menos control puede equivaler a más ignorancia. Disponga de una buena documentación y dedique tiempo a formar a sus clientes internos y externos.

5.3.2. Los principios éticos de los datos federales

https://resources.data.gov/assets/documents/fds-data-ethics-framework.pdf (se visitó el 21 de agosto de 2023)

Los principios éticos de los datos federales ayudan a los usuarios de datos federales a tomar decisiones éticas y promueven la responsabilidad a lo largo del ciclo de vida de los datos: adquisición, procesamiento, difusión, uso, almacenamiento y eliminación. Independientemente del tipo de datos o de su uso, quienes trabajan con datos en el sector público deben tener un conocimiento básico de los principios éticos de los datos. Los dirigentes federales también deben fomentar una cultura basada en la ética de los datos y predicar con el ejemplo. Los principios de la ética de los datos son:

1. Respetar las leyes, reglamentos, prácticas profesionales y normas éticas aplicables

Las leyes existentes reflejan y refuerzan la ética. Por lo tanto, los responsables y usuarios de los datos deben respetar todas las autoridades legales aplicables. Las autoridades legales a menudo abordan situaciones y cuestiones históricas y pueden no seguir el ritmo de la evolución del mundo de los datos y la tecnología. Se anima a los responsables de las organizaciones a mantener unas normas éticas actualizadas y exhaustivas en relación con el uso de los datos.

2. Respetar al público, las personas y las comunidades

Las actividades relacionadas con los datos tienen el objetivo global de beneficiar al bien público. El uso responsable de los datos comienza con una cuidadosa consideración de sus posibles repercusiones. Las iniciativas en materia de datos deben tener en cuenta los contextos locales y comunitarios únicos y aportar un beneficio claro e identificado a la sociedad.

3. Respetar la intimidad y la confidencialidad

La intimidad y la confidencialidad deben protegerse siempre respetando la dignidad, los derechos y la libertad de las personas a las que se refieren los datos. En este contexto, la privacidad es el estado de estar libre de intrusiones injustificadas en la vida privada de las personas, y la confidencialidad es el estado de la información de una persona libre de acceso inapropiado y uso indebido. Un objetivo esencial de la protección de la privacidad y la confidencialidad es minimizar las posibles consecuencias negativas a través de medidas como

la evaluación exhaustiva de riesgos, la prevención de la divulgación y el cumplimiento de las normas de gobernanza de datos. Las actividades relacionadas con la privacidad de las personas deben ajustarse a los Principios de Prácticas Leales de Información (FIPPs).

4. Actuar con honestidad, integridad y humildad

Se espera que todos los líderes federales y usuarios de datos muestren honestidad e integridad en su trabajo con los datos, independientemente de su cargo, función o responsabilidades en materia de datos. Los líderes federales y los usuarios de datos no deben realizar o aprobar comportamientos poco éticos con los datos. Al compartir datos y resultados, el personal debe comunicar la información con precisión y presentar las limitaciones de los datos, los sesgos conocidos y los métodos de análisis aplicables. También debe reconocerse que ningún conjunto de datos puede representar plenamente todas las facetas de una persona, comunidad o problema. Se espera que los líderes federales y los usuarios de datos presenten los datos con humildad, estén abiertos a recibir comentarios y, cuando sea posible, inviten al debate con el público. Además, los usuarios de datos federales deben representar con precisión sus capacidades al trabajar con datos.

5. Responsabilizarse a uno mismo y a los demás

La responsabilidad exige que cualquiera que adquiera, gestione o utilice datos sea consciente de las partes interesadas y se responsabilice ante ellas, según proceda. La rendición de cuentas incluye el manejo responsable de la información clasificada y controlada, el cumplimiento de los acuerdos de uso de datos suscritos con los proveedores de datos, la reducción al mínimo de la recogida de datos, la información a las personas y organizaciones sobre los posibles usos de sus datos, y la posibilidad de acceso público, enmienda e impugnación de los datos y conclusiones, cuando proceda.

6. Promover la transparencia

Las personas, organizaciones y comunidades se benefician cuando el proceso de toma de decisiones éticas es lo más transparente posible para las partes interesadas. La transparencia depende de una comunicación clara de todos los aspectos de las actividades relacionadas con los datos y de un compromiso adecuado con las partes interesadas en los datos. La promoción de la transparencia requiere la participación de las partes interesadas a través de canales de retroalimentación de fácil acceso y el suministro de actualizaciones oportunas sobre el progreso y los resultados del uso de los datos.

7. Manténgase informado de los avances en los campos de la gestión de datos y la ciencia de datos

Las tecnologías avanzadas aportan grandes beneficios al sector público, pero deben desplegarse con un compromiso de rendición de cuentas y mitigación de riesgos. Aunque el uso y el análisis tradicionales de los datos pueden introducir sesgos, los sistemas, tecnologías y técnicas emergentes requieren una mayor concienciación y supervisión porque pueden aumentar las oportunidades de sesgo. Es fundamental mantenerse informado de los avances en los campos de la gestión de datos y la ciencia de datos, especialmente a medida que los métodos avanzados afectan a la recopilación, gestión y uso de datos en el futuro. Además, cada día surgen nuevas innovaciones en materia de datos (por ejemplo, sistemas, soluciones, métodos computacionales), lo que aumenta la importancia de que los dirigentes y empleados federales que trabajan con datos se mantengan al corriente de las innovaciones del mercado y aprendan a utilizar éticamente los nuevos métodos.

5.3.3. Código de ética para el uso de datos en una era de tecnología digital y regulación de McKinsey & Company

https://www.geocities.ws/academia_entorno/eli2.pdf (se visitó el 23 de agosto de 2023)

I.- Introducción

Definición de Profesional de Sistemas: Para efectos del presente código de ética, se entiende dentro del mismo ámbito a las profesiones relacionadas con la informática, la computación y los sistemas computacionales, sea cual fuere su denominación, y se utilizará en lo sucesivo el término *Informático* para definirlo. La lista de normas no es necesariamente exhaustiva y la intención es ilustrar y explicar con detalle el código de ética referente al comportamiento ideal que se espera encontrar en el *Informático*.

II.- Alcance del código de ética

1. Aplicación universal del código. Este código de ética profesional es aplicable a toda persona que tenga una profesión asociada con la informática, la computación o los sistemas

computacionales, sin importar la índole de su actividad o la especialidad que cultive tanto en el ejercicio independiente o cuando actúe como funcionario o empleado de instituciones públicas o privadas.

2. Actuación profesional. El futuro de la profesión del *Informático* depende de la excelencia técnica y ética. Es por eso que se vuelve indispensable que todos los profesionales en esta área se adhieran a los principios ya expresados en este código, así como promover su difusión y práctica.

Los *Informáticos* tienen la ineludible obligación de regir su conducta de acuerdo a las reglas contenidas en este código, las cuales deben considerarse mínimas pues se reconoce la existencia de otras normas de carácter legal y moral, cuyo espíritu amplía el de las presentes.

Este código rige la conducta del *Informático* en sus relaciones con el público en general, con quien patrocina sus servicios (cliente o patrón) y con sus compañeros de profesión, y le será aplicable cualquiera que sea la forma que revista su actividad, la especialidad que cultive o la naturaleza de la retribución que perciba por sus servicios. Los *Informáticos* que además ejerzan otra profesión deben acatar las reglas de conducta incluidas en este código, independientemente de las que señale la organización a la que pertenezcan o presten servicio.

Los *Informáticos* deben abstenerse de hacer comentarios, sobre sus colegas, cuando dichos comentarios perjudiquen su reputación o el prestigio de la profesión en general, a menos que se soliciten por quién tenga un interés legítimo en ellos.

3. Actitud personal. El *Informático* debe respeto a sus semejantes, y su comportamiento en lo personal y social debe atender la práctica de buenas costumbres y seguir un objetivo útil. Debe tener la costumbre de cumplir los compromisos adquiridos, no por el hecho de estar escritos, sino por convicción propia.

El *Informático* debe ser capaz de comprometer su palabra y cumplirla aún en situaciones desfavorables. Además, debe respetar y hacer respetar su tiempo y el de los demás, predicar con el ejemplo, y poseer espíritu de servicio y habilidad para comunicarse con los demás. Actuará siempre cuidando el no afectar la integridad física, emocional ni económica de las personas.

4. Independencia de criterio. Al realizar cualquier proyecto, el *Informático* acepta la obligación de sostener un criterio libre e imparcial, sin aceptar ni permitir presiones de terceros

involucrados en la situación, que pudieran verse beneficiados por la decisión o actitud adoptada.

5. Rechazar tareas que NO cumplan con la moral del profesional de sistemas. El *Informático* hará uso y aplicación de sus conocimientos profesionales sólo en tareas que cumplan con las normas establecidas, y faltará al honor y a la dignidad cuando, directa o indirectamente, intervenga en arreglos o asuntos que no cumplan con las normas establecidas en el "Código de ética del *Informático*".

6. Calidad profesional de los trabajos. En la prestación de cualquier servicio, se espera del Informático un verdadero trabajo de calidad, por lo que se tendrán presentes las disposiciones normativas de la profesión que sean aplicables al trabajo específico que esté desempeñando, y de ser posible, sujetarse a lo más altos estándares de calidad mundial existentes.

7. Preparación y calidad profesional. El *Informático* debe reconocer su nivel de incompetencia y no debe aceptar tareas para las que no esté capacitado. Por ser la información un recurso difícil de manejar en las empresas, se requiere de *Informáticos* que definan estrategias para su generación, administración y difusión, por lo que ninguna persona podrá aceptar un trabajo relacionado con la informática, computación o sistemas computacionales, sin contar con el entrenamiento técnico y la capacidad comprobada necesaria para realizar estas actividades de manera satisfactoria y profesional. El *Informático* vigilará que su propia actualización y capacitación profesional crezca permanentemente.

8. Ejercicio de la profesión. El *Informático* debe tener presente que la retribución económica por sus servicios no constituye el único objetivo ni la razón de ser del ejercicio de su profesión, sino que él mismo se ajustará a los principios humanos en la utilización de la tecnología en bien del avance y desarrollo de la sociedad. Además, debe analizar cuidadosamente las verdaderas necesidades que puedan tenerse de sus servicios, para proponer aquellos que más convengan dentro de las circunstancias.

III.- Responsabilidades hacia el cliente o patrocinador del servicio.

1. La importancia del cliente. El *Informático* debe ubicarse como una entidad de servicio, por lo que su objetivo principal es la atención adecuada al cliente. Debe brindar todo el respeto

al cliente y entender que la única diferencia con él es la formación y habilidad al desarrollar herramientas informáticas, y debe evitar hacer comentarios alabadores al cliente con el objetivo de obtener beneficios, así como evitar hacer comentarios que deterioren la imagen de su cliente por el simple hecho de hacerlo.

2. Proteger el interés del cliente o patrón. El *Informático*, independientemente de cuál sea su relación contractual, debe vigilar por el interés del cliente o patrón y evitar en todo momento crear una situación de dependencia tecnológica hacia sus servicios, y debe alertar al cliente o patrón sobre los riesgos de utilizar cada plataforma de equipos y programas, con respecto a la continuidad de operaciones y servicios, sin la presencia del profesional de sistemas.

El *Informático* debe aprovechar y explotar al máximo las herramientas y aplicaciones adquiridas por la empresa para el beneficio propio de la organización; asimismo, debe indicar cualquier desperdicio de recursos computacionales del cual tenga conocimiento y evitar que la empresa haga gastos innecesarios mediante la utilización adecuada de todos los recursos. También debe informar al cliente o patrón cuando un proyecto propuesto no cumpla con los intereses propios de la organización, así como de cualquier riesgo asociado con el desarrollo de un proyecto que pudiera impactar en el costo, tiempo de entrega o calidad.

El *Informático* no debe aceptar trabajos en los que no se sienta competente para realizarlos a un nivel razonable de satisfacción del cliente. No debe olvidar, en ningún momento, que la satisfacción del cliente es lo más importante, y debe asegurarse del buen uso de los recursos informáticos, evitando desperdiciarlos y gastarlos en formas para las que no fueron planeados y autorizados. Su actitud siempre debe ser en forma pro-activa, para ver más allá de los proyectos que estén a su cargo y buscar mejores soluciones.

3. Responsabilidad profesional. El *Informático* expresará su opinión en los asuntos que se le hayan encomendado, teniendo en cuenta los lineamientos expresados en este código y una vez que haya dado cumplimiento a las normas profesionales emitidas por la organización, que sean aplicables para la realización del trabajo.

Ningún *Informático* que actúe de forma independiente permitirá que se utilice su nombre en relación con proyectos de información o estimaciones de cualquier índole, cuya realización dependa de hechos futuros, en tal forma que induzcan a creer que el profesional de sistemas asume la responsabilidad de que se realicen dichas estimaciones o proyectos.

El *Informático* debe puntualizar en qué consisten sus servicios y cuáles serán sus limitaciones. Cuando en el desempeño de su trabajo se encuentre en alguna circunstancia que

no le permita seguir desarrollando su labor en la forma originalmente propuesta, debe comunicar esa circunstancia a su cliente de manera inmediata. El *Informático* debe ser objetivo e imparcial en la emisión de sus opiniones o juicios buscando siempre el beneficio de sus clientes.

4. Derechos de autor. El *Informático* debe respetar el reconocimiento que hace el Estado a favor de todo creador o desarrollador de programas de cómputo, en virtud del cual otorga su protección para el autor.

Cuando se preste el servicio de modo independiente, el *Informático* debe establecer, en el contrato de servicios, quién será el poseedor de los derechos de autor sobre los programas desarrollados.

Cuando el *Informático* sea el titular de los derechos de autor sobre un programa de computación, tendrá el derecho de autorizar o prohibir el arrendamiento o la venta de sus ejemplares. Podrá tener acceso a las bases de datos con información de carácter privado relativa a personas, previa autorización, excepto cuando se requiera una investigación de carácter legal.

5. Discreción profesional. El *Informático* tiene la obligación de guardar discreción en el manejo de la información que la empresa, para la cual trabaje, le proporcione al momento de prestar sus servicios. Debe considerar como confidencial toda la información acerca del negocio de su cliente o patrón, y debe asegurarse de que se guarde la confidencialidad de la información que le ha sido confiada.

El *Informático* no debe permitir el acceso a la información a personal no autorizado, ni utilizar para beneficio propio la información confidencial de la empresa. Podrá consultar o cambiar opiniones con otros colegas en cuestiones de criterio o de doctrina, pero nunca deberá proporcionar datos que identifiquen a las personas o negocios con los que trate, a menos que sea con consentimiento de los interesados.

6. Honestidad profesional. El *Informático* no debe cambiar, modificar o alterar la información de la empresa para beneficio propio o de terceros, ni con fines de encubrir anomalías, fraudes o corrupción de otros funcionarios que afecten los intereses de la empresa. No debe participar en la planificación o ejecución de actos que puedan calificarse de deshonestos, o que originen o fomenten la corrupción en cualquiera de sus formas, y no aceptará comisiones ni obtendrá ventajas económicas directas o indirectas por la

recomendación que haga de servicios profesionales o de productos a la empresa, institución o dependencia a la que presta el servicio.

7. Lealtad hacia la empresa a la que se le da servicio. El *Informático* se abstendrá de aprovecharse de situaciones que puedan perjudicar a quien haya contratado sus servicios, y observará el principio del secreto profesional.

Siempre que el *Informático* trabaje para un cliente o patrón y que tenga la oportunidad de realizar trabajos profesionales con otros clientes, deberá informar a su patrón original. En caso de tener contrato de planta deberá además cuidarse de no apoyar profesionalmente, directa ni indirectamente, a los competidores de su patrón. No debe ofrecer trabajos directa o indirectamente a funcionarios o empleados de sus clientes, si no es con previo consentimiento del mismo.

El *Informático* en el desarrollo independiente de la profesión debe abstenerse de ofrecer sus servicios a clientes de otro colega; sin embargo, tiene derecho a realizar propaganda y competencia por los distintos medios de difusión, expresando los servicios que ofrece, y si algún cliente que solicita sus servicios está siendo atendido por otro colega, se debe de sugerir la continuación con el colega o la ruptura de esa relación, de tal manera que el cliente solo sea atendido por uno de ellos sobre una misma tarea.

Tratándose de asociaciones profesionales, no podrán los socios contraer o hacer trabajos profesionales por su cuenta, sin el consentimiento de los demás socios.

8. No beneficiarse de las compras del patrón. El *Informático* no debe obtener beneficio económico alguno, directa o indirectamente, cuando lleve a cabo la realización de actividades propias de su profesión dentro de la organización para la que presta sus servicios; no debe buscar su beneficio personal en las compras de equipo y programas realizadas bajo su responsabilidad; no debe ceder a estrategias de soborno por parte de proveedores, y no debe dar consejo, al cliente o patrón, para desarrollar una compra en la cual se pueda ver beneficiado económicamente algún familiar o amigo, a menos que sea con el conocimiento expreso del cliente o patrón.

9. No usar equipo ni programas del cliente o patrón para beneficio personal. Cuando el *Informático* requiera utilizar los equipos de cómputo o programas, propiedad del cliente o patrón para el que se prestan los servicios, para uso personal o de beneficio propio, debe consultar primeramente al propio cliente o patrón y obtener su autorización expresa para tal

fin. No debe usar el equipo propiedad del cliente o patrón para fines de esparcimiento, aún cuando tenga autorización para utilizar el equipo, ni fomentar que personas ajenas a la organización ingresen a las instalaciones para utilizar el equipo y programas.

10. Trato adecuado y manejo del lenguaje apropiado. El *Informático* debe tratar a todas las personas justamente sin tener en cuenta raza, religión, sexo, orientación sexual, edad o nacionalidad. Debe dar a sus colaboradores el trato que les corresponde como profesionales y vigilará su adecuado entrenamiento, superación y justa retribución. No debe intentar confundir o engañar al cliente con comentarios técnicos mal fundamentados respecto a los sistemas computacionales, para lograr beneficio propio o enmendar fallas o errores propios.

11. Finalización de servicios. Al finalizar un proyecto, el *Informático* debe cumplir con todos los requisitos de funcionalidad, calidad y documentación pactados inicialmente, a fin de que el cliente pueda obtener el mayor beneficio en la utilización de los mismos. Al dejar la empresa para la cual se prestaban los servicios, el *Informático* debe cuidar que el equipo de cómputo y los programas propiedad de la empresa se conserven en buen estado para su uso y aprovechamiento. Al concluir el trabajo para el cual fue contratado, debe implementar los mecanismos necesarios para que el cliente esté en posibilidad de continuar haciendo uso de los programas de aplicación, modificaciones o novedades que hubiere realizado a los mismos, a pesar de la ausencia del *Informático*.

12. Dependencia tecnológica. El Informático debe evitar en todo momento generar una dependencia tecnológica con el cliente o patrón, siguiendo estándares de desarrollo de software adecuados al cliente u organización para la cual se prestan los servicios. Debe apegarse a los estándares de calidad en el análisis, diseño y programación de sistemas, y facilitar en todo momento la comprensión por parte de terceros de su participación en el desarrollo de un sistema.

IV.- Responsabilidad hacia la profesión

1. Respeto a los colegas y a la profesión. Todo *Informático* cuidará las relaciones que sostenga con sus colaboradores, colegas e instituciones buscando el enaltecimiento de la profesión, actuando con espíritu de grupo y trabajo en equipo. Debe cimentar su reputación en la honestidad, honradez, lealtad, respeto, laboriosidad y capacidad profesional, observando las

reglas de ética más elevadas en sus actos y evitando toda publicidad con fines de lucro o autoelogio. Buscará pertenecer a un Organismo Colegiado que cuente con un Código de Ética que se haga respetar y cumplir. En caso de no existir cuerpos colegiados de informática en su localidad, fomentará su creación y posteriormente la adopción de un código de ética.

2. Imagen de calidad. El *Informático* debe esforzarse por mantener una imagen positiva y de prestigio para quien lo patrocine y ante la sociedad en general, fundamentada en su calidad profesional e individual.

3. Difusión y enseñanza de conocimientos. Todo *Informático* debe mantener altas normas profesionales y de conducta, especialmente al transmitir sus conocimientos; así como contribuir al desarrollo y difusión de los conocimientos de la profesión.

4. Respeto a los derechos de autor. El *Informático* reconoce los derechos de autor sobre todos los programas de aplicación, desarrollados por colegas o empresas afines, y se compromete a protegerlos y a evitar que otros hagan uso de los mismos sin antes haber pagado por tales derechos.

5. Especialización profesional. El *Informático* debe tener una orientación hacia cierta rama de la informática, computación o sistemas computacionales, debiéndose mantener a la vanguardia en esa área del conocimiento de su particular interés.

6. Competencia profesional. Es obligatorio para el *Informático* mantener actualizados todos los conocimientos inherentes a las áreas de su profesión, así como participar en la difusión de estos conocimientos a otros miembros de la profesión. Debe informarse permanentemente sobre los avances de la informática, la computación y los sistemas computacionales, además de invertir los recursos necesarios para su capacitación y formación profesional y personal.

7. Evaluación de capacidades. El *Informático* debe autoevaluarse periódicamente con la finalidad de determinar si cuenta con los conocimientos, tiempo y recursos que requiere su cliente. En caso de que el *Informático* tenga empleados a su cargo, deberá asegurarse de que las capacidades técnicas de sus empleados o subordinados sean evaluadas periódicamente, al mismo tiempo que se debe asegurar de que cuentan con un código de ética como el presente.

8. Reconocimiento a la colaboración profesional. El *Informático*, al consultar a otro colega, debe ser consciente del esfuerzo, trabajo y recursos que su colega ha dedicado al dominio de los diferentes programas y equipos de cómputo, estando dispuesto en todo momento a retribuir los honorarios adecuados por la asesoría solicitada.

9. Honorarios. El *Informático* debe ser capaz de practicar un procedimiento para costear sus proyectos que le permitan, con seguridad, establecer sus honorarios sin necesidad de hacer cambios posteriores; debe establecer cuotas justas al fijar sus honorarios y debe respetarlos una vez que fueron acordados con sus clientes; debe de establecer perfectamente el tiempo y la forma de pago, y debe evitar establecer honorarios por debajo de los costos reales.

10. Personal a sus servicios. El *Informático* debe realizar una supervisión del desempeño del personal que colabore con él en el desarrollo de proyectos. Debe hacerse totalmente responsable del personal que colabore con él en el desarrollo de proyectos, cuando tal personal no sea del cliente.

11. Conflicto de intereses en la profesión. El *Informático* debe evitar recibir favores de los clientes a cambio de beneficiarlos en forma personal, con tratos preferenciales a futuro. Debe evitar cualquiera de las acciones siguientes: establecer relaciones sentimentales con los clientes, influir en los clientes para que tomen decisiones que posteriormente lo beneficien personalmente, el acoso hacia el cliente, e influir en crear u otorgar puestos que puedan ser ocupados por sus familiares o amigos dentro de la organización del cliente.

V.- Uso de Internet

1. Normas generales para su uso. Es obligación imperativa e ineludible del *Informático*, en todas las ocasiones en las que navegue en Internet, portarse con honor y dignidad, ajustándose a la más estricta moralidad, velando por el prestigio personal, decoro profesional y actuando con decencia en todos los casos.

Por el prestigio y buen uso de Internet, el *Informático* debe observar las reglas de este código de ética cuyas infracciones, por considerarse actos indignos y punibles, serán actos reprobatorios. Además, es su obligación fomentar y hacer que los usuarios de la red cumplan estas mismas normas, para evitar que el Internet pierda prestigio.

2. Creación y uso de páginas en Internet. El *Informático* entiende que son actos contrarios a este código de ética, los siguientes:

- Navegar en páginas de Internet contrarias a las buenas costumbres, como páginas pornográficas o páginas con contenido insano, entre otras.
- Crear páginas de Internet sabiendo que contienen mentiras, falsedades y que se realizan con dolo, y hacer creer a los usuarios que lo que contienen es verídico.
- Dejar páginas en Internet abandonadas sin cumplir con lo que se promete en ellas.
- Crear páginas con mala promoción a terceras personas, ya sean físicas o morales, con el fin de perjudicarlos.
- Ofrecerse para el desempeño de especialidades y funciones para las cuales no se tiene capacidad, preparación y experiencia razonables.
- Crear páginas con virus para que al momento de bajar algún archivo este sea enviado al usuario.
- Comercializar el software libre en Internet.
- Leer, modificar, borrar o dañar información de otros usuarios con dolo o en forma accidental.
- Establecer enlaces a páginas sin estar debidamente autorizado a hacerlo y cumpliendo con los derechos de autor involucrados en dichos enlaces.

3. Correo electrónico. El *Informático* entiende que son actos contrarios a este código de ética, los siguientes:

- Enviar correos electrónicos conteniendo injurias, falsedades y malas palabras, aunque el usuario sea de mucha confianza.
- Enviar correos electrónicos sin remitente y sin asuntos.
- Enviar, por correos electrónicos, virus, archivos o información que vaya en contra de las buenas costumbres.
- Enviar correos electrónicos SPAM a los usuarios.
- Enviar, a través de correo electrónico, publicidad no solicitada por el usuario.
- Enviar correos electrónicos haciéndose pasar por otra persona.
- Solicitar el correo electrónico de una persona con la finalidad de enviarle, por una sola vez, información solicitada, y posteriormente enviarle información no solicitada.
- Enviar correos electrónicos a los contactos de otros usuarios sin su autorización expresa.

▪ Usar el correo electrónico, de la empresa en la que trabaje, para asuntos personales sin contar con previa autorización para hacerlo.

6. Conclusiones

Uno de los resultados del trabajo, si no el principal, parece ser que, examinados los nuevos campos profesionales surgidos de la redefinición de la Información y Documentación en Gestión Digital de la Información y la Documentación, se puede concluir que todavía no hay propiamente códigos éticos y/o deontológicos sino más bien manuales de buenas prácticas, lo que es lógico porque es un campo en consolidación conceptual, económica, social, y hasta legal, según se desprende de la revisión y análisis de algunos de los principales documentos disponibles en España, Reino Unido y Estados Unidos. En realidad, la conclusión general del trabajo es la confesión y aceptación de que habrá que seguir observando la evolución del campo profesional. Todo esto confirma que es correcta la hipótesis planteada inicialmente. Con respecto a la comparativa, tras la revisión y el análisis de estos documentos se observa que Reino Unido, en comparación con España y Estados Unidos, es el país que posee los manuales de buenas prácticas más completos.

En cuanto a los principios de protección de datos, España presenta un manual escueto, cuyas indicaciones son ampliadas en el manual de Reino Unido, y en lo que respecta a Estados Unidos, este país no posee un manual de principios de protección de datos como tal. Uno de los principios de protección de datos de España (en el caso de España se denominan principios fundamentales del Derecho a la Protección de Datos), es el de que los datos personales solamente podrán ser tratados de forma lícita, leal y transparente, y este principio está también indicado en la Ley de protección de datos de 2018 de Reino Unido, aunque en este último caso se explica cuándo el tratamiento es lícito, leal y transparente. Esta última ley establece que, para determinar si el tratamiento de datos personales es leal y transparente, se tendrá en cuenta cómo se obtienen esos datos, y se consideran obtenidos de forma leal y transparente si consisten en información obtenida de una persona que esté autorizada, por ley, a suministrarla, o que esté obligada a suministrarla en virtud de una ley o de una obligación internacional del Reino Unido.

Reino Unido, en su Ley de protección de datos de 2018, también amplia el otro principio de protección de datos de España, que es el de legitimación. España establece, simplemente, que

se debe informar al titular de los datos, con absoluta claridad, sobre cuáles son las finalidades para las que se recogen sus datos. Reino Unido indica que esta finalidad debe ser específica, explícita y legítima, y que los datos personales no deben tratarse de forma incompatible con la finalidad para la que se recogen. España establece en el manual "Los principios de la ética de los datos", sin embargo, que las empresas y las organizaciones deben ser transparentes en cuanto a la finalidad de la recopilación y almacenamiento de los datos. Reino Unido también emplea el concepto "transparencia" en su "Guía para la Ciencia de Datos Ética", indicando que los profesionales deben ser transparentes y honestos a la hora de comunicar cómo se utilizan los datos. Estados Unidos no habla de transparencia como tal, pero sí que indica, en el manual "Los principios éticos de los datos federales", que se debe informar a las personas y organizaciones sobre el posible uso de sus datos.

En Reino Unido, si se están utilizando datos personales, hay que cumplir los principios del Reglamento General de Protección de Datos de la UE (GDPR) y la Ley de Protección de Datos de 2018 (DPA 2018). El artículo 35 del GDPR establece que es obligatorio realizar una evaluación del impacto sobre la protección de datos (DPIA) cuando sea probable que haya un riesgo alto para los derechos de las personas, en particular cuando se usen nuevas tecnologías. España cuenta con el Reglamento General de Protección de Datos, cuyo artículo 13 incluye toda la información que se debe proporcionar a las personas interesadas cuando se recogen sus datos personales. En Estados Unidos, las actividades relacionadas con la privacidad de las personas deben ajustarse a los Principios de Prácticas Leales de Información (FIPPs).

Con respecto al uso de los datos, Reino Unido, concretamente en el manual "La ética del Big Data", habla de una serie de conceptos, relacionados entre sí, que no son mencionados en ningún manual de los otros dos países. Estos conceptos son el consentimiento informado, el consentimiento amplio y el consentimiento escalonado. El consentimiento informado es la forma más respetuosa, cuidadosa y ética de consentimiento, y requiere que la persona que recopila los datos haga un gran esfuerzo para explicar razonablemente y con precisión, a las personas participantes, cómo se utilizarán sus datos. El consentimiento amplio y el consentimiento escalonado son dos revisiones de la norma del consentimiento informado. El consentimiento amplio autoriza, de forma previa, los usos secundarios de los datos. El consentimiento escalonado autoriza usos secundarios específicos de los datos; por ejemplo, para la investigación del cáncer, pero no para la investigación genómica. Reino Unido es el único de los tres países que introduce estos conceptos; sin embargo, cabe señalar que algunos expertos argumentan que tanto el consentimiento amplio, como el consentimiento escalonado, exponen a los usuarios a prácticas poco éticas.

Unos conceptos que prácticamente solo están presentes en uno de los manuales de Reino Unido, son el sesgo y la objetividad de los algoritmos. El susodicho manual, "La ética del Big Data", explica estos conceptos diciendo que los algoritmos son diseñados por humanos, que los algoritmos solamente estudian conjuntos de datos seleccionados y preparados por humanos, y que los humanos tienen prejuicios. Además, afirma que existen pruebas significativas que sugieren que la tecnología y los algoritmos están siendo infectados por los prejuicios humanos, y estos prejuicios están causando daño en las personas, sobre todo las que pertenecen a grupos minoritarios. Se hace unas pequeñas menciones del concepto de sesgo en el caso de Estados Unidos, en el manual "Los principios éticos de los datos federales", afirmando que los sistemas, las tecnologías y las técnicas emergentes pueden aumentar los niveles de sesgo, por lo que requieren una mayor concienciación y supervisión, e indicando que los/las profesionales deben presentan los sesgos conocidos cuando compartan datos y resultados. En cuanto a los manuales españoles, no hacen mención alguna de los conceptos de sesgo y objetividad de los algoritmos.

España concuerda con Reino Unido y Estados Unidos en varios aspectos. Coincide con Reino Unido en que los datos personales deben tratarse de forma lícita, leal y transparente; en que se debe ser transparente a la hora de comunicar cómo se utilizan los datos, y en que se deben adoptar medidas de seguridad para que personas no autorizadas accedan a los datos, aunque Reino Unido especifica que son datos personales. Concuerda con Estados Unidos en que se debe respetar la propiedad intelectual.

España es el único de los tres países que posee un manual para la profesión *Community Manager* y que, además, explica claramente la diferencia entre "seguridad de los datos" (cuestión técnica) y "privacidad de los datos" (cuestión legal); sin embargo, necesita incluir conceptos y explicaciones que sí están incluidos en los manuales de los otros dos países, especialmente en el caso de Reino Unido. Debe: explicar mejor sus principios de protección de datos, como hace Reino Unido; incluir, al igual que Reino Unido, la obligación de evaluar el impacto sobre la protección de datos cuando sea probable que exista un riesgo elevado para los derechos de las personas, e incluir y explicar los conceptos de sesgo y objetividad de los algoritmos, como sí llevan a cabo Estados Unidos y, sobre todo, Reino Unido.

Bibliografía

(http://www.agpd.es), AEPD, and ISMS Forum (http://www.ismsforum.es). "Código De Buenas Prácticas En Protección De Datos Para Proyectos Big Data." 2017. https://www.aepd.es/es/documento/guia-codigo-de-buenas-practicas-proyectos-de-big-data.pdf.

Adelstein, Jennifer, and Stewart Clegg. "Code of Ethics: A Stratified Vehicle for Compliance." *Journal of Business Ethics* 138 (2016): 53-66.

Barcelona, Universitat de. "Grado En Gestión De Información Y Documentación Digital." https://web.ub.edu/es/web/estudis/w/grado-G1098?subjects.

Bentham, Jeremy. *Deontología O Ciencia De La Moral.* 2 vols. Valencia: Librería de Mallen y sobrinos, 1835.

Bentham, Jeremy, and Amnon Goldworth. *Deontology ; Together with a Table of the Springs of Action ; and the Article on Utilitarianism.* Oxford: Clarendon Press, 1983.

Ceplis. "Los Valores Comunes De Las Profesiones Liberales En La Unión Europea. Versión Revisada-2014." Bruselas, 2014. https://ceplis.org/common-value/.

Corcuera, Pablo, and Leticia Ponce de León G. "Tendencias De Los Movimientos Conservacionistas Y El Surgimiento De La Eco-Ética." *Sociológica México*, no. 56 (2015): 199-211.

Delgado-Alemany, Rafael, Alicia Blanco-Gónzalez, and María-Ángeles Revilla-Camacho. "Códigos Deontológicos: El Rol De Los Colegios Profesionales Y Las Profesiones Reguladas." *Revista ESPACIOS.ISSN* 798 (2020): 1015.

"Deontología Profesional. Los Códigos Deontológicos." Unión Profesional, 2009. https://unionprofesional.com/estudio/deontologia_profesional/.

Documentación, Facultade de Humanidades e. "Grado En Gestión Digital De Información Y Documentación." https://humanidades.udc.es/estudos/gdid/informaci%C3%B3n-del-t%C3%ADtulo.

Escudero Muñoz, Juan M. "Un Cambio De Paradigma En La Formación Continuada Del Profesorado: Escenario, Significados, Procesos Y Actores." (2020).

Estado, Jefatura del. "Ley 2/2007, De 15 De Marzo, De Sociedades Profesionales." 2007. https://www.boe.es/buscar/act.php?id=BOE-A-2007-5584.

García Fernández, Ángel. "Ética Y Deontología." *Educación y biblioteca* 19, no. 159 (2007): 67-75.

Helin, Sven, and Johan Sandström. "An Inquiry into the Study of Corporate Codes of Ethics." *Journal of Business Ethics* 75 (2007): 253-71.

Infoeducación.es. "Listado De Profesiones Reguladas En España Divididas Por Áreas." https://infoeducacion.es/profesiones-reguladas-espana/.

Lere, John C., and Bruce R. Gaumnitz. "Changing Behavior by Improving Codes of Ethics." *American Journal of Business* 22, no. 2 (2007): 7-18.

Lugli, Ennio, Ulpiana Kocollari, and Chiara Nigrisoli. "The Codes of Ethics of S&P/Mib Italian Companies: An Investigation of Their Contents and the Main Factors That Influence Their Adoption." *Journal of Business Ethics* 84 (2009): 33-45.

Madrid, Universidad Carlos III de. "Grado En Gestión De La Información Y Contenidos Digitales." https://www.uc3m.es/grado/contenidos-digitales#programa.

Martín Sánchez, David. "La Construcción De La Ecoética En España Y La Proyección De Futuro De Su Aplicación Laboral Mediante La Deontología Ambiental." *Observatorio medioambiental*, no. 25 (2022): 179-98.

Murcia, Universidad de. "Grado En Gestión De Información Y Contenidos Digitales." https://www.um.es/web/estudios/grados/contenidos-digitales.

Múzquiz Vicente-Arche, Gonzalo. *La Función Deontológica De Las Organizaciones Colegiales Y Su Impacto Económico Y Social.* Unión Profesional (Madrid: 2016). https://unionprofesional.com/estudio/la-funcion-deontologica-de-las-organizaciones-colegiales/.

"¿Qué Son Los Colegios Profesionales Y Para Qué Sirven? Conócelo En 5 Puntos." Unión Profesional, 2021. https://unionprofesional.com/cuadernillos/.

Rodríguez Ruiz, Juan Roger. *Ética Profesional Y Deontología.* Universidad Católica Los Ángeles de Chimbote, 2015.

Schwartz, Mark. "The Nature of the Relationship between Corporate Codes of Ethics and Behaviour." *Journal of Business Ethics* 32 (2001): 247-62.

Velayos Castelo, María Carmen. "La Ecoética En España." *La albolafia: revista de humanidades y cultura*, no. 2 (2014): 129-51.

Verde-Diego, Carmen, and Óscar Cebolla Bueno. "Deontología Profesional: La Ética Denostada." *Cuadernos de trabajo social* 30, no. 1 (2017): 77.