Ética, Legislación y Profesión

"'Aprender"' a hacer tu trabajo de una fomra ética y legal

Alejandro Barrachina Argudo

Grado en Ingeniería informática
Facultad de Informática
Universidad Complutense de Madrid

2022-2023

Índice general

1 | Introducción a la Ética y la Legislación

1.1. Introducción a la Ética

La ética es una parte de la filosofía, la cual implica cuestionarse sobre problemas relativos al bien, al deber, a la virtud o al vicio. Los objetivos de la ética son:

1. Llegar a alguna conclusión acerca de lo que es correcto o no
2. Que la conclusión pueda ser defendida con argumentos.
3. Justificar las normas que regulan el comportamiento en diferentes ámbitos de la vida

La reflexión es la consideración minuciosa de un asunto, esto implica dedicarle tiempo y no quedarse con la primera impresión. Para llevar a cabo esta consideración minuciosa debemos:

- Informarnos: contrastar fuentes y poder citarlas.
- Pros y contrastar.
- Partes afectadas.
- Circunstancias.
- Posibles escenarios futuros.
- Contrastar: comentar, dialogar, escuchar otros puntos de vista diferentes al propio.
- Discernir, analizar

Es importante hacerse muchas preguntas para poder reconocer y tener en cuenta a todas las partes implicadas, dirigir esfuerzos a la hora de buscar información, ampliar nuestra visión del tema y compartir o hacer esas preguntas a otras personas para ampliar nuestra perspectiva. Los elementos claves para una reflexión ética son:

1. Identificar los valores del conflicto.
2. Empatía: personas/colectivos afectados: ponerse en el lugar de los otros, percibir a los demás como seres sintientes.
3. Analizar las circunstancias.
4. Pros, contras y su peso.
5. Alcance de las consecuencias en el espacio y el tiempo.
6. Posibles escenarios futuros partiendo del presente.

Tras una reflexión ética debemos llegar a una conclusión clara, directamente relacionada con los argumentos y ejemplos reales utilizados. Esta conclusión debe ser coherente con los argumentos y ejemplos usados. Si esta conclusión está matizada demostrará un correcto proceso de reflexión.

1.2. Introducción a la Legislación

El derecho es la técnica de dar a cada persona lo que le corresponde. También es un conjunto de normas organizadas, escritas o no, cuyo cumplimiento es obligatorio y pueden ser impuestas de forma coactiva, que sirven para asegurar la pacífica convivencia.

El Código Civil en su art. 1.1 señala como fuentes del Derecho:

1. La Ley: norma vigente.
2. La costumbre: conductas repetidas desde tiempos inmemoriales. Solo rige en defecto de ley aplicable y siempre que no contradiga la moral o al orden público y tiene que ser probada.

3. Los PGD (Principios Generales del Derecho): principios fundamentales. Se aplican en defecto de la Ley o costumbre. Además, su contenido está siempre presente en el ordenamiento jurídico.

Estas fuentes de derecho tienen una jerarquía, lo que hace que una disposición no carezca de valor si contradice a una de rango superior. Ley > costumbre > PGD. La legislación refleja una serie de valores (Derechos, protección) y una serie de conflictos (delitos, sanción, penas).

1.3. Cuestiones éticas relacionadas con el diseño de aplicaciones informáticas

Tanto el diseño como el software son políticos, ya que podemos considerar que "Los algoritmos son opiniones incrustadas en código".

El diseño de un software no es neutro, ya que se tienen que considerar distintos puntos al hacer el programa:

- Qué función o funciones realiza.
- Qué restricciones ponemos al usuario y cuales no.
- Qué datos vamos a recolectar y/o analizar.
- Qué podemos deducir sobre los usuarios.
- Qué mecanismos se van a utilizar para crear o no adicción entre los usuarios.

Un ejemplo de software político puede ser BOSCO, una aplicación financiada por el Gobierno Español utilizada por las compañías eléctricas para decidir quién tiene derecho a un descuento en la factura de la luz.

Otro ejemplo sería el sistema VeriPol utilizado por la Policía Nacional para detectar denuncias falsas.

1.3.1. Manipulación online

Algunos de los casos más conocidos son: Facebook con su publicidad dirigida a adolescentes estresados y deprimidos, Uber con estrategias para conseguir que sus conductores trabajen más horas o en determinadas zonas y Cambrige Analytica y sus mensajes políticos personalizados basados en perfiles de Facebook.

Dentro de la manipulación online podemos ver varios tipos:

- **Persuasión (influencia):** cualquier forma de influencia e influencia a través de la discusión racional.
- **Persuasión en sentido explicito:** es visible, consciente y resistible (hay alternativas).
- **Manipulación:** es oculta, inconsciente y explota vulnerabilidades cognitivas emocionales y estructurales o individuales. La víctima no es consciente de que ha sido dirigida a una decisión determinada. Hay un beneficio para la parte manipuladora.
- **Manipulación + TIC (Tecnologías de la información y la comunicación):** hay grandes cantidades de información personal y algoritmos que analizan estos datos que son invisibles y omnipresentes. Generan campañas individualizadas con anuncios y mensajes a medida.

Estas acciones pueden producir daños materiales como gastar dinero en cosas que no necesitamos o gastar más de lo que queríamos o daños en cuanto a violación de la autonomía, con impacto individual y/o social y político.

Al estudiar un programa tenemos que hacernos las siguientes preguntas:

- Quién decide qué y cómo se diseñan.
- Si tiene mayor o menor potencial manipulador.
- Si está diseñada para ser adictiva.
- Si está diseñada para potenciar el comportamiento impulsivo y disminuir la capacidad analítica.
- Si se da al usuario una falsa sensación de autonomía.

1.3.2. El salto a la IA

La evolución de la IA nos ha traído sistemas muy complejos con aprendizajes profundos (encuentran patrones en un conjunto de datos) que sacan conclusiones estadísticas y son fáciles de engañar.

Al ser entrenadas mediante conjuntos de datos, £Pueden sus diseñadores predecir su comportamiento? Algunas arquitecturas de IA funcionan como una caja negra en la que no sabemos el porqué de las decisiones de la máquina, aunque no todas las arquitecturas son tan opacas.

Hay que tener en cuenta el hecho de que el sesgo cognitivo y los prejuicios de los desarrolladores de una IA pueden influir de manera negativa en su toma de decisiones. Estos sesgos pueden ser inconscientes o heredados(por el diseño o por el conjunto de datos que se usa para el entrenamiento) o prejuicios deliberados que nazcan de una determinada política o idea.

Para evitar IAs con este tipo de problema tenemos que buscar siempre que el algoritmo sea explicable.

> Cómo asegurar que el algoritmo es justo, cómo asegurar que el algoritmo es interpretable y explicable: todo eso está todavía bastante lejos.
>
> *Nihar Shah*

Es de interés para las personas que desarrollan el algoritmo, para abogades y jueces y para toda la ciudadanía entender la toma de decisiones de un algoritmo.

Parte de evitar problemas de bias viene en forma de auditorías, para las cuales hay que tener acceso a:

- Diseño: explicabilidad, trazabilidad y reproducibilidad.
- Datos de entrenamiento o conjunto de datos para probar el sistema.
- Código fuente

1.3.3. Guía ética para una IA confiable (UE)

> To everyone who shapes technology today
> We live in a world where technology is consuming society, ethics, and our core existence. It is time to take responsibility for the world we are creating. Time to put humans before business. Time to replace the empty rhetoric of building a better world with a commitment to real action. It is time to organize, and to hold each other accountable.
>
> *The Copenhagen Letter, 2017*

La UE define una IA fiable como una que es lícita, ética y robusta. Una IA fiable debe respetar cuatro principios éticos (a parte de respetar los derechos fundamentales):

- Respeto de la autonomía humana.
- Prevención del daño.
- Equidad.
- Explicabilidad.

Una IA fiable debe cumplir también siete requisitos clave:

- Acción y supervisión humanas.
- Solidez técnica y seguridad.

- Transparencia.
- Diversidad, no discriminación y equidad.
- Bienestar social y ambiental.
- Rendición de cuentas.

Para aplicar estos principios hay que hacerlo desde el propio diseño del algoritmo: poniendo el respeto al ser humano por encima de cualquier otro tipo de interés como centro del diseño, respetar la autonomía individual y colectiva, no discriminar, revisar los sesgos, hacer un algoritmo explicable y transparente, respetar la privacidad y los DDAA (derechos de autor) (licencia y opciones de protección de los DDAA) y prever y tratar de evitar posibles usos fraudulentos y/o delictivos del algoritmo.

2 | Privacidad

2.1. Derecho fundamental

La privacidad es un derecho fundamental recogido en la Constitución Española de 1978 en el Articulo 18:

1. Se garantiza el derecho al honor, a la intimidad personal y familiar y a la propia imagen.
2. El domicilio es inviolable. Ninguna entrada o registro podrá hacerse en él sin consentimiento del titular o resolución judicial, salvo en caso de flagrante delito.
3. Se garantiza el secreto de las comunicaciones y, en especial, de las postales, telegráficas y telefónicas, salvo resolución judicial.
4. La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos.

2.2. Redes sociales

Las redes sociales tienen diseños basados en crear adicción (modelo "Hooked" de Mil Eyal), con técnicas de persuasión/ manipulación / coacción y extracción de datos del usuario para su monetización.

Los términos y condiciones de una red social recogen datos importantes como:

- Copyright
- Información que recogen y cómo la almacenan:
  - Qué información.
  - Donde (transferencia de datos fuera de la UE).
  - Durante cuánto tiempo.
  - Con quién la comparten.
  - Para qué la utilizan.
- Cambios, notificaciones.
- Como cerrar una cuenta y que pasa con ella después de cerrarla,
- Cookies de rastreo
- Censura de contenido

Pero normalmente la gente no las lee, ya que son largas y complicadas con mucho texto jurídico. Es importante leer estos términos de servicio para ser conscientes de lo que hace la aplicación con nuestros datos.

Es importante también saber que una clausula o termino ilegal no tiene validez aunque aparezca en los términos de servicio y que toda empresa que opere en la UE debe cumplir con el RGPD

El auge de las redes sociales a traído también el ciberacoso, que tiene un mayor impacto y difusión que el acoso "tradicional". Podemos decir que hay tres tipos de ciberacoso: exclusión, manipulación y hostigamiento, también podemos diferenciar tres partes: persona que acosa, persona que es acosada y persona observadora.

El ciberacoso puede causar una reacción en cadena, ocasionando un efecto de bola de nieve. No hay violencia física pero causa un perjuicio muy grande en la víctima.

Al usar las redes sociales es importante pensar en qué uso damos de ellas, cuánto las usamos y si las usamos de manera correcta. Es importante el impacto de nuestros actos en las redes sociales.

2.3. LOPD y RGPD

El RGPD se define en el Reglamento (UE) **2026/679** del Parlamento Europeo y del Consejo de 27 de abril de 2016 y es relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE.

La LOPD es una adaptación de este reglamento en nuestro país, cada país miembro tiene su propia adaptación.

El RGPD define su entrada en vigor y aplicación en el **Artículo 99**:

- El presente Reglamento entrará en vigor a los veinte días de su publicación en el Diario Oficial de la Unión Europea.
- Será aplicable a partir del 25 de mayo de 2018.

El presente reglamento será obligatorio en todos sus elementos y directamente aplicable en cada Estado miembro.

El esquema del RGPD es:

1. 173 consideraciones (28 páginas): por qué, para qué (preámbulo).
2. Disposiciones Generales.
3. Ámbito de aplicación: actividades realizadas en la UE independientemente de donde realices el tratamiento.
4. Definiciones
5. Principios: relativos al tratamiento, al consentimiento, definir categorías especiales de datos personales etc.
6. Derechos: transparencia, información y acceso, rectificación, oposición + art. 17 → Derecho al olvido.
7. Limitaciones: casos judiciales etc.
8. Obligaciones de responsables del tratamiento.

2.3.1. Consideraciones

1.- La protección de las personas físicas en relación con el tratamiento de datos personales es un derecho fundamental. El Artículo 8, apartado 1, de la Carta de los Derechos fundamentales de la UE y el Artículo 16, apartado 1, del TFUE (Tratado de funcionamiento de la Unión Europea) establecen que toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan.

6.- La rápida evolución tecnológica y la globalización han planteado nuevos retos para la protección de datos personales. La magnitud de la recogida y del intercambio de datos personales ha aumentado de manera significativa. La tecnología permite que tanto las empresas privadas como las autoridades públicas utilicen datos personales en una escala sin precedentes a la hora de realizar sus actividades. Las personas físicas difunden un volumen cada vez mayor de información personal a escala mundial.

58.- El principio de transparencia exige que toda información dirigida al público o al interesado sea concisa, fácilmente accesible y fácil de entender, y que se utilice un lenguaje claro y sencillo, y, además, en su caso, se visualice. Esta información podría facilitarse en forma electrónica, por ejemplo, cuando esté dirigida al público, mediante un sitio web. Ello es especialmente pertinente en situaciones en las que la proliferación de agentes y la complejidad tecnológica de la práctica hagan que sea mas difícil para el interesado saber y comprender si se están recogiendo, por quién y con qué finalidad, datos personales que le conciernen, como es en el caso de la publicidad en línea.

83.- A fin de mantener la seguridad y evitar que el tratamiento infrinja lo dispuesto en el presente Reglamento, el responsable o el encargado deben evaluar los riesgos inherentes al tratamiento y aplicar medidas para mitigarlos, como el cifrado.

Estas medidas deben garantizar un nivel de seguridad adecuado, incluida la confidencialidad, teniendo en cuanta el estado de la técnica y el coste de su aplicación con respecto a los riesgos y la naturaleza de los datos personales que deban protegerse.

101.- En todo caso, la transferencia a terceros países y organizaciones internacionales solo pueden llevarse a cabo de plena conformidad con el presente Reglamento.

Una transferencia solo podría tener lugar si, a reserva de las demás disposiciones del presente Reglamento, el responsable o encargado cumple las disposiciones del presente Reglamento relativas a la transferencia de datos personales a terceros países u organizaciones internacionales.

2.3.2. AEPD

La AEPD es el organismo público encargado de velar por el cumplimiento de la LOPD en España.

La AEPD lista los siguientes derechos del ciudadano sobre sus datos:

- Derecho a conocer: para qué se usan tus datos, plazo de conservación, derecho a presentar una reclamación ante la AEPD y la existencia de decisiones automatizadas, elaboración de perfiles y sus consecuencias.
- Derecho a solicitar al/la responsable: suspensión del tratamiento de tus datos, conservación de tus datos, portabilidad de tus datos a otros proveedores de servicios.
- Derecho a rectificar tus datos: cuando sean inexactos o cuando estén incompletos.
- Derecho a suprimir tus datos: por tratamiento ilícito, por desaparición de la finalidad que motivó el tratamiento o recogida, cuando revocas tu consentimiento o cuando te opones a que se traten.
- Derecho a oposición al tratamiento de tus datos: Por motivos personales, salvo que quien trata tus datos acredite un interés legítimo, cuando el tratamiento tenga por objeto el marketing directo.

La AEPD también ofrece una "Guía para responsables de tratamiento de datos" en la cual se establecen unos principios a seguridad

El principio de responsabilidad proactiva. Este principio exige una actitud consciente, diligente y proactiva por parte de las organizaciones frente a todos los tratamientos de datos personales que se lleven a cabo. Este principio requiere que las organizaciones analicen qué datos tratan, con qué finalidades lo hacen y qué tipo de operaciones de tratamiento llevan a cabo. A partir de este conocimiento deben determinar de forma explícita la forma en la que aplicarán las medidas que el RGPD prevé, asegurándose de que esas medidas son las adecuadas para cumplir con el mismo y de que pueden demostrarlo ante los interesados y ante las autoridades de supervisión. Podemos distinguir seis medidas de responsabilidad activa:

- Análisis de riesgos
- Registro de actividades de tratamiento
- Protección de datos desde el diseño y por defecto
- Medidas de seguridad
- Notificaciones de "violaciones de seguridad de los datos"
- Evaluaciones de impacto sobre la Protección de datos

Todos los responsables deberán realizar una valoración del riesgo de los tratamientos que realicen, a fin de poder establecer qué medidas deben aplicar y cómo deben hacerlo. El tipo de análisis variará en función de: el tipo de tratamiento, la naturaleza de los datos, el número de interesados afectados y la cantidad y variedad de tratamientos que una misma organización lleve a cabo.

Responsables y encargados deberán mantener un registro de operaciones de tratamiento en el que se contenga la información que establece el RGPD y que contenga cuestiones como:

- Nombre y datos de contacto del responsable o corresponsable y del Delegado de Protección de Datos si existiese.
- Finalidades del tratamiento.
- Descripción de categorías de interesados y categorías de datos personales tratados.
- Transferencias internacionales de datos.

Están exentas las organizaciones que empleen a menos de 250 trabajadores, a menos que el tratamiento que realicen pueda entrañar un riesgo para los derechos y libertades de los interesados, no sea ocasional o incluya categorías especiales de datos o datos relativos a condenas e infracciones penales.

Protección de Datos desde el Diseño y por Defecto. Estas medidas se incluyen dentro de las que debe aplicar el responsable con anterioridad al inicio del tratamiento y también cuando se esté desarrollando.

Este tipo de medidas reflejan muy directamente el enfoque de responsabilidad proactiva. Se trata de pensar en términos de protección de datos desde el mismo momento en que se diseña un tratamiento, un producto o servicio que implica el tratamiento de datos personales.

Cuando se produzca una violación de seguridad de los datos, el responsable debe notificar a la autoridad de protección de datos competente, a menos que sea improbable que la violación suponga un riesgo para los derechos y libertades de los afectados.

La notificación de la quiebra a las autoridades debe producirse sin dilación indebida y, a ser posible, dentro de las 72 horas siguientes a que el responsable tenga constancia de ella. Los responsables del tratamiento deberán realizar una EIPD (Evaluación de Impacto sobre la Proteccin de Datos) con carácter previo a la puesta en marcha de aquellos tratamientos que sea probable que conlleven un riesgo alto para los derechos y libertades de los interesados.

Glosario

AEPD Agencia Española de Protección de Datos

DDAA derechos de autor

EIPD Evaluación de Impacto sobre la Proteccin de Datos

IA Inteligencia Artificial

LOPD Ley Orgánica de Protección de Datos

PGD Principios Generales del Derecho

RGPD Reglamento General de Potección de Datos

TFUE Tratado de funcionamiento de la Unión Europea

TIC Tecnologías de la información y la comunicación

UE Unión Europea

Índice de figuras

Índice de cuadros

Licencia de uso del documento

Licencia de uso del código fuente

Los archivos de código fuente para generar este documento se encuentran en `https://github.com/alk222/ELP` bajo la licencia GPL-3.0