Tema 9. TIC, Sociedad, Profesión y Ética: una confluencia necesaria.

Tienes que saltar siempre por el precipicio y construir las alas en el camino de descenso.

Ray Bradbury

Una vez asentadas las bases de la ética y deontología informática vamos un paso más lejos: nuestra sociedad, donde todos vivimos, cambia. Y nosotros no somos ajenos a esos cambios, que sufrimos por acción u omisión. Hablaremos del fenómeno hacker, particularizando en lo que se ha dado en llamar "hacking ético" y en fenomenologías con una incidencia cada vez mayor, como la llamada "ciberguerra" o las actuaciones basadas en la ingeniería social. Tras ello, visitaremos a vuelapluma fenómenos tan presentes como la inteligencia artificial, la robótica, el Internet de las Cosas o el Big Data colocando el acento en nuestro trabajo, todo ello sin dejar de particularizar las referencias que ya vimos sobre los códigos éticos.

Introducción

Hay unas cuantas figuras que brillan con luz propia en lo que se ha dado en llamar el submundo informático. Una de ellas es la cada vez más mediática de Kevin Mitnick. Pues bien, una frase recogida de uno de sus libros es la que parece dar la clave de lo que a continuación trataremos de desarrollar. Dice Mitnick que "desde mi punto de vista, en el colegio deberían enseñar a los niños los principios de la ética informática desde la escuela primaria, cuando se inician en el uso de ordenadores" (Mitnick & Simon, 2007).

Efectivamente, el ordenador ya no es tan solo un electrodoméstico más, es algo que forma parte del ADN de cualquier sociedad de hoy, y no solo algo accesorio, sino un elemento central. Y ya que a todos se nos pide que nos comportemos y mantengamos unas buenas formas, e incluso para usar herramientas peligrosas (como puede ser un coche) nos certifiquemos para poder usarlo (siguiendo el ejemplo, el carnet de conducir), parece lógico esperar que, desde niños, seamos instruidos en las "buenas formas".

Uno de los problemas principales es donde fijar el punto de vista ético: esos valores que se supone debemos compartir. Podemos pensar que en el común uso, en lo que es habitual, aunque en ocasiones, es algo desacertado. Se sabe que la interacción en línea precisamente reafirma conductas no deseables. Así, un pederasta que no tenga comunicación con otros de su calaña, puede finalmente caer en que su actitud es reprobable. Pero si tiene la retroalimentación positiva de un grupo de personas como él, el grupo puede hacerle sentir más fuerte y pensar que no es tan malo eso que hace. Esa motivación que aparece no siempre es mala: cuando el objetivo es bueno, el colaborar al realizar determinadas prácticas brinda la oportunidad de respaldar acciones consideradas positivas y el compromiso. Dudley aquí mete una cuña planteando que podemos pensar que la participación en las actividades de al-Qaeda, en línea o en la vida real, tiene poco de virtuoso, y. sin embargo, el efecto conseguido por la

colaboración online de estos terroristas o aprendices de terroristas es que se reafirman unos a otros en que esa idea común es positiva (Dudley, Braman, & Vincenti, 2012).

Por otra parte, atendiendo a la figura del "hacker" (término que por la claridad y su popularización emplearemos sin comillas), es sabido que no todos son lo que podríamos catalogar como hermanitas de la caridad. Ejemplos hay muchos, pero el más típico es el que nos da Libicki: Los hackers también pueden entrar en los sistemas empresariales, haciéndose pasar por usuarios legítimos con los derechos y privilegios de cualquier otro usuario (Libicki, 2009). Por otra parte, veremos en este mismo tema que su empleo como personal de alta cualificación forma parte ya del día a día de los estados modernos. Hablaremos sobre como aparecen guerras de baja intensidad, a partir de confrontaciones políticas entre estados o grupos, con un perfil de hostilidad inferior a la guerra convencional, pero que al tiempo supera la convivencia pacífica entre naciones.

Las TIC afectan en toda la órbita del ser humano: familia, tocio u trabajo. Esa sociabilidad digital influye en la profesionalidad del individuo no es la menos importante: la presencia de amigos en su entorno de trabajo suele implicar que una persona trabaje más o menos duro que en caso de estar sola; bien por no parecer un sabelotodo, echa el freno, y así de paso evita que le consulten de continuo, o, si es alguien un tanto lento, o directamente holgazán, puede intensificar su quehacer para así evitar parecer un perezoso. En cualquier caso, las relaciones humanas, que es el libro sobre el que se escribe la ética, afectan a su capacidad de trabajo. ¿Parece exagerado? Pensemos que la manipulación en base a los ejemplos externos y a las influencias que de fuera vienen, está a la orden del día. Esto se ve de forma gráfica con un ejemplo: pensemos en el mundo del espectáculo, donde cada año el nivel de lo que es aceptable o moral parece cambiar, vendiéndosenos el cambio como "libertad". Esos cambios proceden de lo que "el público", esa masa anónima aplaude con sus audiencias o deja de hacerlo. Finalmente el individuo, parte de la masa, es manipulado por la masa en sí misma, y termina cambiando en muchos casos sus propios criterios (Hadnagy, 2011).

Y por supuesto, nos queda algo que parece que es nuevo, pero no lo es tanto, la Inteligencia Artificial (IA), y la robótica. Si preguntamos si queremos tener un robot, la mayoría diríamos que sí, y se trata de una mayoría qué en realidad no sabe que ya los tiene, incluso nadie diría que él mismo podría llegar a ser un robot por hibridación en el futuro. Si preguntamos si nos gustaría ser transportados en taxi sin conductor o compartir nuestros trabajos con un robot, probablemente la mayoría dirá que no si se lo piensa un poco. Hay un trasfondo ético pero también jurídico. (Barrio Andrés, 2018) . Esto nos llevará a considerar la intersección de las TIC con los valores humanos[1].

Es algo evidente que las sociedades actuales han entrado en una dinámica de cambio constante, lo cual a su vez implica, como nos recuerda (Colmenarejo Fernández, 2017) la

[1] : Los elementos a considerar según (Bynum & Rogerson, 2004) serían:

1. Relaciones humanas
2. Privacidad y anonimato
3. Propiedad intelectual
4. Trabajo
5. Justicia social
6. Gobierno y democracia.

necesidad urgente de desarrollar una ética adaptada los cambios que provocan los avances tecnológicos sobre la calidad y las formas de vida. Y es que hay años luz entre saber jugar al ajedrez y sentir el corazón en un puño al escuchar una ópera de Verdi (Latorre Sentís, 2019). Pero ¿y si hablamos componerlo? Recordemos sistemas como DeepBach[2]. Quizá no estemos tan lejos del futuro como creemos, sino ya dentro de él. Y es que… pensar el futuro es el primer paso para habitarlo. (Latorre Sentís, 2019)

Un poco de historia.

No podemos dejar de dar unas pinceladas sobre los hitos históricos en la ética de la informática: Seguimos para ello a (Bynum & Rogerson, 2004) y lo exponemos para mayor simplicidad de forma lineal.

- 1940 a 1950. Norbert Wiener y su obra, en particular "The human use of Human Beings".
- 1960. Donn Parker examinó los usos ilegales y poco éticos de los profesionales de la informática, se le considera tras Norbert Wiener el segundo padre de la ética informática.
- 1970. Joseph Weizenbaun crea ELIZA, programa informático diseñado en el MIT, fue uno de los primeros programas en procesar lenguaje natural. Escribió "Computer Power and Human Reason" (1976), siendo considerado una persona clave en la ética informática. El término Computer ethics lo crea a mitad de los años 70 Walter Maner definiéndolo como el campo aplicado en las éticas donde los problemas pueden ser agravados, transformados o creados por la tecnología de los ordenadores.
- 1980 a 1990. James Moore publicó su artículo "what is computer ethics?" en 1985. También hay que considerar la obra de Sherry Turkle en 1984, "The Second Self"

Definiciones

Vamos a apuntar una serie de términos que nos serán precisos para el desarrollo del tema actual. Empecemos con lo más básico, la ética informática. Para ello nos haremos eco de la

[2] Hice un experimento empleando composiciones "al estilo de" Vivaldi, Beethoven y Bach. Generadas por una IA y, puestas a prueba con humanos, no advertidos de su origen, las dudas se decantan entre si son piezas poco conocidas de los compositores o de coetáneos.

No hace mucho se cifraba el verdadero salto de la IA no en conseguir máquinas que vencieran intelectualmente a los humanos, algo que ya ha sucedido hace tiempo, o que lograran sustituirlos en tareas intelectualmente complejas (p.e. como radiólogos en hospitales, lo que ya ha sucedido también), sino en el sentir, como dice Latorre, el corazón en un puño al escuchar a Verdi.

Y puede que sea un error, ya que todos conocemos que una parte importante de nuestra sociedad que no se emociona ni ante Verdi, ni ante Velázquez, ni ante absolutamente nada, sea la muerte de un niño, una tragedia en Nepal o la muerte de su propia madre. Tras ese camino que hemos recorrido como sociedad, donde nuestros dirigentes no han sido precisamente inocentes, creo que si, en breve, la IA nos superará. Y me permito apostillar: ¿y a quien le importa? Algunas direcciones que ilustran esto (no referenciadas a modo de bibliografía, sino como ejemplo)

https://www.youtube.com/watch?v=CgG1HipAayU
https://www.youtube.com/watch?v=o7zTLw7s2dc
https://www.youtube.com/watch?v=2kuY3BrmTfQ
https://www.youtube.com/watch?v=QiBM7-5hA6o

evolución histórica del concepto, siguiendo el estudio de (Bynum & Rogerson, 2004). Se enmarcan cinco etapas, que pueden verse en la tabla siguiente.

Tabla 1 Evolución del concepto "ética informática", según Bynum & Rogers

1	Maner fue el primero en usar el término de computer ethics a mediados de la década de 1970 como "problemas éticos agravados, transformados o creados por la tecnología informática".
2	En su libro, Computer Ethics (1985), Deborah Johnson lo definió como "estudio de nuevas actitudes morales ante problemas y dilemas. Incremento de antiguos problemas, y obligación de crear de forma ordinaria normas morales inexploradas".
3	En su artículo "¿Qué es la ética informática?" (1985), James Moor proporcionó una definición de ética informática que es mucho más amplia y más amplia que las de Maner o Johnson. Es independiente de cualquier teoría filosófica específica; y es compatible con una amplia variedad de enfoques para la resolución ética de problemas. Desde 1985, la definición de Moor ha sido la más influyente. Definió la ética informática como un campo relacionado con "vacíos de políticas" y "confusiones conceptuales" con respecto al uso ético y social de la tecnología de la información. Un problema ético surgiría por no existir políticas sobre cómo usar un ordenador. Nos dan nuevas capacidades y esto nos fuerza a dar determinados giros a las acciones que ya teníamos consolidadas. Junto con un vacío de políticas, a menudo hay un vacío conceptual.
4	En 1989, Terrell Ward Bynum siguiendo una sugerencia en Moor, usó una definición basándose en identificar y analizar impactos tecnológicos en lo social y humano (salud, riqueza, trabajo, oportunidad, libertad, democracia, conocimiento, intimidad, seguridad, realización personal, etc.)
5	En la década de 1990, Donald Gotterbarn cambió el prisma. Para él la ética informática debiera ser vista como una rama de la ética profesional profesional, preocupado ante todo con estándares de buenas prácticas y códigos de conducta para informáticos profesionales

Otros términos que nos harán falta, para complementar los del tema anterior, serán:

Cibernética: del vocablo griego kybernetes, que significa piloto o timonel. En Platón, kybernetiké expresa propiamente el arte del pilotaje y, a su vez, extensivamente, el arte de gobernar a los hombres. Del término griego - kyberneter; kybernetes- procede la voz latina gubernator, que tiene aproximadamente la misma significación griega. Las lenguas neolatinas recogen del latín la voz y la significación: en español tenemos, por ejemplo, por una parte, gobernalle, término náutico y, por otra, gobierno, gobernador, término político y administrativo. En 1834, el célebre científico André Marie Ampère en su conocido ensayo sobre la filosofía de las ciencias, emplea la voz cybernetique para indicar el estudio de los medios de gobierno, en la política. (David, 1973). Con todo esto, entendemos plenamente la definición que la Real Academia da del término: Ciencia que estudia las analogías entre los sistemas de control y comunicación de los seres vivos y los de las máquinas.

Inteligencia artificial: Toda técnica de procesamiento de información caracterizada por hacer cálculos sobre determinada información en un espacio dimensional virtual y construido mediante operaciones generalmente no lineales llevadas a cabo dentro del propio algoritmo

para aprovechar diversas propiedades de espacios altamente dimensionales. (Barrio Andrés, 2018)

Robot: es de sobra conocido su origen de la mano del autor de ciencia ficción Karel Čapek. La Real Academia lo define como: máquina o ingenio electrónico programable, capaz de manipular objetos y realizar operaciones antes reservadas solo a las personas. Pero nos interesa más un término derivado, la **roboética**, que se define como la parte aplicada de la ética cuyo objetivo es el desarrollo de herramientas técnico-científicas y culturales que promuevan la robótica como causa de avance de la sociedad humana y de sus individuos y que ayuden a prevenir un uso equivocado de ésta contra la propia especie humana. (Barrio Andrés, 2018)

Muy ligado a lo anterior aparece un término cada vez más frecuente, la **máquina ultrainteligente**: aquella que puede superar en todas las actividades intelectuales a cualquier humano, por listo que este sea. Dado que el diseño de máquinas es una de estas actividades, una máquina ultrainteligente podría diseñar máquinas aún mejores. Incuestionablemente, habría una explosión de inteligencia, y la inteligencia humana quedaría totalmente rezagada. En consecuencia, la primera máquina ultra inteligente será la última invención que los hombres podrán hacer, asumiendo que esa máquina sea suficientemente dócil como para permitir que mantengamos su control. (Latorre Sentís, 2019)

Ética informática y profesional informático

Ya hemos visto que a pesar de ser la Informática una ciencia reciente, es una de las ciencias centrales en la actualidad, pues es de las que más influencia ha tenido a lo largo del siglo XX, como queda claro en algo ya manido: se suele comparar su impacto con la Revolución Industrial, pues ha cambiado la forma de pensar y actuar no solo de las personas sino de los grupos sociales. (Garriga Domínguez, 2012). Los trabajadores de esa disciplina tienen pues una serie de responsabilidades que cada vez se hacen más importantes para el conjunto de la sociedad. Aunque no siempre fue así.

Relacionar la ética dentro de la profesión informática es algo que surge de manera estructurada y con entidad científica en la década de los 90 del pasado siglo. Tal y como (Himma & Tavani, 2008) dicen y hemos adelantado en este tema, en esos años Donald Gotterbarn defendía que la ética informática debía ser vista como la ética profesional dedicada al desarrollo y avance de las normas de buenas prácticas y códigos de conducta para los profesionales de la informática. De ésta manera, y como uno de los puntos de partida, en 1991 publica su artículo "Ética de la computación: la responsabilidad recuperada", de donde destacamos el siguiente párrafo: "Hay poca atención al campo de la ética profesional, a los valores que guían en el día a día las actividades de los trabajadores de la informática en su papel como profesionales. Por profesional de la informática me refiero a cualquier persona involucrada en el diseño y desarrollo. Las decisiones éticas realizadas durante el desarrollo tienen una relación directa con muchos de los temas tratados en el marco del más amplio concepto de ética de la computación". Gotterbarn es una de las figuras clave, trabajó con un comité de la ACM para la creación de su "Código de Ética y Conducta Profesional" y con otros miembros de la ACM y de la Computer Society del IEEE, cuyos códigos éticos referenciamos en el apartado pertinente.

Esta visión, muy ligada al desarrollo, es compartida por otros autores. Así, (Bynum & Rogerson, 2004), dedican el capítulo 6 de su obra a la ética en la gestión de un proyecto software, asunto de sumo interés que trataremos en este mismo apartado. Pero quizá pecaría de miopía una visión de la ética en la profesión informática sin tratar otros aspectos, como los que reseñamos a continuación.

Por una parte tenemos la esfera de la relación del trabajador con su empresa. Edgar (Edgar, 2003) habla de la lealtad que el trabajador le debe a la empresa, salvo cuando descubre que la empresa hace cosas ilegales e inmorales (el tan conocido "Whistle Blowing"). También Edgar habla de los errores en el ejercicio de sus funciones y la responsabilidad que se contrae con ellos. La catalogación de posibles errores es enorme (cambio de identidades, errores de transcripción...) y variable según el tipo de puesto y organización donde se desempeñe. Hay lugares, como por ejemplo en aquellos relacionados con la medicina, donde éstos pueden ser si no más graves, si más visibles socialmente. Sobre éste tema en concreto pueden consultarse casos (Khosrow-Pour, 2003) (revisado en 2007), (Barger, 2008), y reflexiones diversas (Himma & Tavani, 2008). Sin embargo, otros, (Cotino, 2008) relacionan exclusivamente éste tema con la ley y, como mucho, recomendaciones de la Unesco.

Otro factor importante, reseñado por (De George , 2003), en su capítulo 3, y por (Edgar, 2003) es el control de las comunicaciones que el trabajador tiene dentro de la empresa (e incluso en ocasiones, fuera): correos que pueda enviar o recibir, webs que visite, presencia en redes sociales y uso de las mismas... y, sobre todo, lo importante que resulta que existan grabaciones o logs de esto.

Sería absurdo intentar abarcar todas las facetas posibles, que son muchas y diversas, sobre todo teniendo en cuenta la transversalidad de la profesión informática: podemos encontrar informáticos en hospitales, colegios, fuerzas y cuerpos de seguridad del estado, bancos, empresas farmacéuticas... cada puesto de trabajo tendrá unos cuantos aspectos comunes y otros tantos propios e intransferibles. Pero si podemos destacar una serie de elementos fundamentales en la ética de las TIC y los negocios. Esto lo veremos con detalle en su apartado correspondiente, pero podemos empezar con uno de los autores ya citados y comprobaremos que, si no están todos los elementos de interés, al menos si son de interés todos los elementos citados: (De George , 2003).Así, menciona como principal para un trabajador del sector la privacidad, el riesgo que corre o puede hacer correr, las relaciones dentro del llamado e-business con todo lo anterior, el peligro de que la flexibilidad en el mundo laboral qué se produce con las TIC, esto es, elementos como teletrabajo, tiempo flexible, globalización, sistemas expertos, se vuelva en contra y por último, la censura (que De George relaciona con la pornografía, especialmente la infantil)

Tampoco podemos esperar que aparezca sola. Lamentablemente, la ética no surge de manera natural en una organización, por lo que es preciso emprender una serie de acciones para incorporar esos comportamientos. Reischl nos dice que "la tecnología no es ni moral ni inmoral, porque no es ni buena ni mala". De acuerdo, pero ¿puede decirse lo mismo de las personas que están detrás de la tecnología y la venden? Al decir esto, habla de Google, aunque podría subirse a este carro otro tipo de empresas, como Facebook, por ejemplo (Reischl, 2008) (otra visión de interés en (Ippolita, 2010)). Y es que hay una doble moral que no se puede

obviar. El ejemplo lo da Suarez Sánchez-Ocaña al referirse a como Telecinco y su guerra contra Youtube, ya que mientras en algunos programas emitía vídeos de Youtube, denunciaba la subida de fragmentos de sus programas en la plataforma (Suarez Sánchez-Ocaña, 2012).

La ética en los proyectos informáticos.

(Bynum & Rogerson, 2004) plantean la cuestión mediante un par de pasos, partiendo del presupuesto de que se trata de una actuación correcta. Para determinar esto, ofrecen una batería de preguntas que deben tener un resultado monocolor. Si el asunto es afrontable, es cuando se establece un plan: enumeran los principios básicos que un profesional de las TIC debe moverse, con cuestiones que nos permiten saber si vamos o no por buen camino y esto se cruza de forma matricial con los pasos de un proyecto informático. Vamos a ver esto punto a punto. Empecemos con las preguntas.

- ¿La acción final dará como resultado algo positivo? Para obtener resultado, se plantea la siguiente batería de preguntas sobre la acción a ejecutar:
- ¿Es honorable? : ¿Hay alguien de quien te gustaría ocultar la acción?
- ¿Es honesta?: ¿Viola algún acuerdo, real o implícito, o de otro modo traiciona un compromiso?
- ¿Evita la posibilidad de conflicto de intereses? : ¿Hay otras consideraciones que puedan sesgar el juicio?
- ¿Está dentro de su área de competencia? : ¿Es posible que incluso con tu mejor esfuerzo el resultado no sea adecuado?
- ¿Es justo? ¿Es perjudicial para los intereses legítimos de los demás?
- ¿Es considerado? ¿Va a violar la confidencialidad o privacidad o dañar a alguien o algo?
- ¿Es de naturaleza conservadora? ¿Se desperdicia innecesariamente el tiempo u otros recursos valiosos?

Para ser ética según (Bynum & Rogerson, 2004), una acción debe provocar una respuesta positiva a todas las preguntas anteriores aplicables y una respuesta negativa a cada explicación.

Una vez vemos que no hay problema, dejamos de verlo de forma general y lo particularizamos. Para ello, se establece una relación de principios éticos para profesionales de la informática.

Tabla 2 Principios éticos para profesionales de la informática, adaptado de Bynum y Rogerson.

Principio	Pregunta relacionada
Honor	¿La acción se considera más allá de todo reproche?
Honestidad	¿La acción violará algún acuerdo explícito o implícito?
Sesgo	¿Hay alguna consideración externa que pueda sesgar la acción a tomar?

Adecuación profesional	¿Está la acción dentro de los límites de nuestra capacidad?
Cuidado debido	¿Se usan los mejores estándares de garantía de calidad posibles?
Equidad	¿Se consideran todos los puntos de vista de los implicados con respecto a la acción?
Consideración (Costo social)	¿Se acepta la responsabilidad y la responsabilidad que conlleva esta acción?
Acción efectiva y eficiente	¿Es la adecuada dados los objetivos establecidos, y se usa el menor gasto de recursos?

Por último, dados los pasos de desarrollo de un proyecto, se vincula a cada uno de estos pasos una relación de estos principios.

Tabla 3 Principios éticos dominantes en cada paso de la gestión de un proyecto. Adaptación de Bynum y Ward

Paso/principio	Honor	Honestidad	Sesgo	Adecuación	Cuidado	Equidad	Consideración	Acción
Visualizar el objetivo	X	X	X		X	X	X	
Lista de los trabajos que deben			X					X
Asegurarse de que haya un líder			X	X	X			X
Asignar personas a los trabajos	X	X	X	X				X
Gestionar las expectativas		X			X	X	X	
Estilo de liderazgo	X			X			X	X
Controlar lo que sucede								X
Contar lo que sucede	X	X	X		X	X		

Repetir los pasos anteriores hasta realizar el objetivo					X			X
Realizar el objetivo del proyecto	X		X				X	X

Con la tabla precedente podemos saber dónde debemos marcar el foco en cada uno de los pasos.

Deberes del profesional informático

Ya tenemos al profesional dentro de un proyecto. Nos queda marcar esas delicadas líneas rojas que no debe traspasar. Para ello, seguimos a (Vázquez & Barroso, 1996) que nos dan la relación siguiente:

Secreto profesional

Nace de un contrato tácito o expreso entre aquel que ejerce la profesión de informática y aquel que acude en busca de su consejo en virtud de su profesión. La materia del secreto profesional se extiende a todo aquello que no puede por su naturaleza, ser manifestado sin causar perjuicio justificado y, además, a todo cuánto ha sido confiado bajo promesa de guardar silencio. Para informáticos se extiende no solamente a lo que ha sido confiado directamente al profesional, sino a todo aquello que ha llegado a conocimiento del profesional en virtud de la exploración o datos que se le han dado directamente. Por nuestras manos pasan muchos datos que implican no solo la privacidad de las personas, sino muchas veces su vida en sí. Se ha hablado mucho del poder que da la informática, algo que parte del clásico de Orwell 1984, con su Gran Hermano, y llega a nuestros actuales sistemas de prevención de delito con algoritmos "Pre-Crimen" o al mismo Big Data.

Habría que relacionar esto con la fidelidad a la institución o empresa y el whistle bowling que ya anticipábamos.

La dicotomía

Se refiere a trabajar con varias "caretas", a la división horarios, a la repartición indebida o fraudulenta de honorarios… es una práctica moralmente ilícita, se trata de repartir los honorarios de la consulta, dar comisiones etc.

Soborno

Dar ventajas o regalos de todo tipo para conseguir determinadas concesiones o contratos en favor de terceras personas o entidades.

Relaciones laborales

Se atenta contra la deontología en las relaciones laborales al incumplir un contrato laboral, por tema salarial, tanto por ser excesivamente bajos en las escalas más modestas como por excesivamente elevados para los altos directivos, por abusar de trabajadores eventuales, por aumentar los beneficios por procedimientos condenables, cuando se producen bajos rendimientos que ocasionan costes, cuando se dan quiebras culpables y fraudulentas o escándalos financieros, o cuando no se adoptan garantías efectivas en trabajos proclives al

riesgo y, en general, todo aquel tipo de trabajo que no sea adaptado a las actitudes fuerzas y capacidades de la persona según edad sexo y salud.

Dentro de esas relaciones laborales habría que considerar la prevención del delito. Parece paradójico tras haber planteado la discusión sobre los algoritmos pre-crimen como demasiado intrusivos, pero es que hablamos no de inferir conductas sobre las personas, sino en la prevención pura. Lo cierto es que aprovechando una red que gestionemos, un empleado puede cometer delitos informáticos que no solo caerán sobre nuestra conciencia, sino sobre nuestro expediente: si un empleado usa las redes de la empresa para hacer spam, para amenazar a alguien, para propagar contenidos peligrosos, nos aseguramos al menos una visita de las fuerzas y cuerpos de seguridad. A este respecto, cabe recomendar la lectura de un caso magníficamente expuesto por Jennings: "Employee and Technology Privacy: Is the Boss Spying?" (Jennings, 2009).

También las TIC parecen empujar a continuar trabajando a personas que deberían estar jugando o comunicándose con su familia y amigos. La frontera familiar, la invasión de la privacidad y el ocio, mantener los límites: familia, trabajo y diversión. De igual forma que los juegos online o las redes sociales captan cada vez a más personas, el teletrabajo puede afectar en el mismo sentido. Ese es otro aspecto que encajaría dentro de las llamadas relaciones laborales.

Además de lo que dejan sentado (Vázquez & Barroso, 1996) nos permitimos añadir un elemento de interés adicional.

Vigilancia tecnológica

Hay algunos aspectos de las TIC que preocupan a la sociedad en general. Al margen de elementos como la brecha digital, los analfabetos digitales, que ya se intentan combatir desde nuestra legislación, consideramos facetas de honda preocupación sobre la que todo profesional debe estar alerta.

En este sentido podríamos hablar del fenómeno "cyberbullying" o el "revenge porn", de su prevención pero como algo que va más allá de impedir un delito, sino de poner toda barrera posible para combatirlos, hablamos de un nivel mucho más elevado. Pensemos que elementos como el porno de la venganza, o el acoso, puede llevar a las personas a casos extremos que incluso consideren el suicidio. Vamos a poner acento en dos elementos muy sensibles: las "fake news" y la información de menores.

Empecemos con las llamadas "**fake news**", que son una edición corregida y aumentada de los viejos chismes y mentiras de portería pero que cobran una importancia tremenda con la red de redes. Pensemos en la facilidad que hay para, usando rumores, decantar la balanza política de un país o hundir a una empresa. La primera duda es ¿por qué nos lo tragamos? Y la explicación viene casi de nuestra propia evolución. El ser humano durante casi toda su historia, mejor dicho, la prehistoria, antes de registro escrito alguno, vivió en comunidades, en tribus, muy pequeñas. Cuando llegaba una noticia del estilo "el león viene corriendo", le dábamos la credibilidad que necesitaba nuestra vida para ser salvada. Dividíamos el mensaje por el número de gente que podía darlo. Si en una tribu de 20 individuos, cuatro nos avisaban de la llegada del león, una probabilidad del 20% era muy alta: el león venía.

Ahora nos llega miles de veces la noticia de que el león viene, y además es verde y con topos violetas. Pero seguimos dividiendo por el número de gente conocida, que es mucha, pero no es todo el globo. El mensaje, si llega muchas veces, sigue siendo creíble. Como además el ser humano tiene, como todos los antropoides, una innata tendencia a imitar, se produce inmediatamente el contagio en la red: todos empiezan a copiar. Y provoca el éxito de las teorías conspiranoicas: sí da la impresión de que todo el mundo está hablando de algo, eso debe ser cierto.

En particular es de mucho interés el poner cuidado en los **niños**. Nos recuerda (Livingstone, 2009) que cada vez es más fácil crear contenidos, no solo por profesionales, sino por los mismos niños, que muchas veces no le dan por sí mismos el significado y las consecuencias del uso de Internet. En este sentido, Livingstone nos ofrece una tabla con oportunidades y riesgos de las actividades online para menores. (Livingstone, 2009)

Tabla 4 Oportunidades y riesgos online, adaptado de Livingstone.

Oportunidades	**Riesgos**
Acceso global a la información	Contenidos ilegales
Recursos educativos	Pederastas
Redes sociales entre amigos	Violencia extrema o sexual
Entretenimiento, juegos y diversión	Otro contenido ofensivo dañino
Aprender a desarrollar contenidos	Material y actividades racistas
Participación cívica o política	Publicidad y marketing agresivo
Privacidad ante la propia identidad	Información errónea o parcial
Participación en la comunidad / activismo	Robo de información personal
Incremento de conocimientos tecnológicos y alfabetización digital	Acoso / acoso cibernético / Cyber-bullying
Mejoras para futuros empleos	Juegos de azar
Orientaciones sobre salud / sexo	Phishing, estafas financieras
Foros especialistas	Autodaño (suicidio , anorexia)
Foros de fans	Inducción a cometer actividades ilegales
Compartir experiencias con otros	

Los niños usan las oportunidades, es cierto. Exploran espacios privados online para experimentar con nuevas identidades, para buscar anuncios confidenciales, explorar gustos personales, inspeccionar la interacción de los otros o para conocer personas de lugares lejanos. A pesar de que la charla online puede aparecer vacua para los observadores adultos,

para los niños es una actividad altamente valorada socialmente, convirtiéndose en la generación del contacto constante. (Livingstone, 2009). Pero como también hay riesgos, hay que prevenirlos. Livingstone matiza la relación anterior con una clasificación de riesgos online para los niños.

Tabla 5 Riesgos online para los niños, adaptado de Livingstone.

	Engaños comerciales	Daño directo	Sexo	Falsos valores
Contenido – niño como recipiente	Anuncios Spam Patrocinadores	Violencia Contenido con carga de odio	Pornografía o contenidos sexuales inesperados	Racismo Consejos engañosos (p.e. drogas)
Contacto – niño como participante	Seguimiento / recolección de información personal	Ser intimidado, acosado.	Conocer extraños, pederastas	Autolesión, Incomodas charlas
Conducta - niño como actor	Juegos de azar, descargas ilegales.	Acosar a otro	Crear y subir pornografía.	Facilitar adicciones o malas conductas (p.e. suicidio, posturas pro-anoréxicas)

Dimensiones morales

¿Cómo podríamos clasificar los elementos principales en torno a los cuales agrupar los dilemas que suscitan los sistemas de información? Si revisamos la literatura científica podemos encontrar una cantidad de clasificaciones tal que necesitaríamos todo el espacio de los apuntes de la asignatura para simplemente reseñarlas. Vamos simplemente a dejar constancia de las más clásicas y luego nos centraremos en la que, por su completitud, nos parece más relevante, las dimensiones morales de los profesores Laudon (Laudon & Laudon, 2016). De hecho, queda como propuesta para el lector el ver como todas las categorías que van apareciendo encajan en una de las dimensiones morales, que se ven con más detalle.

Un texto de referencia presente en toda relación que se precie es el de (Bynum & Rogerson, 2004), quienes aluden a los aspectos de las relaciones humanas que se afectan por la intersección de ética e informática. Así, hablan de temas tales como

- El cibersexo.
- La privacidad y el anonimato. Relacionado con el punto relativo a la privacidad, se plantean si los políticos y otros personajes públicos deben gozar de una privacidad asimilable a la del resto de los ciudadanos.

- La propiedad intelectual, de forma amplia, desde la difusión de material multimedia a los múltiples frentes que se abren, de los que conviene destacar la dicotomía entre cultura y propiedad.
- Relaciones laborales, incluyendo el teletrabajo y sus problemas.
- Posibles problemas de justicia social. Éste es un tema muy amplio, que va desde el analfabetismo digital hasta a gente sin identidad digital que puede perder toda identidad.
- Gobierno y democracia: del voto electrónico al contacto de los ciudadanos con sus representantes, un tema que las redes sociales han vuelto a colocar en el candelero.

Es una visión más próxima a lo que nosotros buscamos: crear categorías por su interacción con el ser humano y la sociedad en general. Otros autores, como (Edgar, 2003) lo que hacen es tomar la ley como referencia, lo que si bien ha sido tomado como un eje vertebrador por muchos, pensamos que nos aleja de lo que es nuestro propósito al hablar de ética, de deontología: se trata de ir más allá de lo que la ley exige. Así, parte de la división de daños realizados contra los ordenadores o usando ordenadores y relaciona:

- Estafa (un usuario no que existe realiza una compra).
- Robo de servicio (servicios de telecomunicaciones).
- Robo de información (mediante sniffers, por ejemplo).
- Fraude (lucrarse mediante engaño. Esto es muy amplio, obviamente. Básicamente hablamos de dos cosas: presentar información falsa para obtener beneficio o, directamente, malversar).
- Crimen organizado, donde el autor incluye el fenómeno de la pederastia.
- "Counterfeiting" o falsificación: robo de cuentas, la suplantación de perfiles…

Como hemos anticipado, vamos a centrarnos para el desarrollo en el trabajo de los profesores Laudon. Sus dimensiones morales de los sistemas de información son una propuesta clásica (su primera edición es de 1996) para enfrentarse a la ética de los sistemas de información. Son cinco categorías en las que encajarían todos los dilemas a los que un profesional puede enfrentarse: (1) derechos y obligaciones de la información, (2) derechos y obligaciones de propiedad, (3) calidad del sistema, (4) calidad de vida y (5) rendición de cuentas y control. Vamos a ir desgranándolos.

Derechos y obligaciones de información:

¿Qué derechos de información poseen los individuos y las organizaciones con respecto a sí mismos? ¿Qué pueden proteger? Podríamos hablar de campos tan actuales como Big Data o el IoT (a través de la información de los sensores)

Ya sabemos que en España, en la UE, esto es un derecho básico, recogido en la normativa sobre Protección de Datos, donde además se habla con algo que entra de lleno en el campo de la ética, los *códigos tipo*. También nos incumben en este sentido aspectos como el control del correo electrónico en las organizaciones.

Los algoritmos cruzan datos y buscan sacar conclusiones entre las personas y sus comportamientos y personas. Aquí aparece el primer punto: ¿Es ético crear programas que recopilan información sobre nuestro comportamiento? ¿Hasta qué nivel es lícito que el

humano sea supervisado, analizado, escudriñado en sus detalles más íntimos por legiones de programas operados por intereses que desconocemos? (Latorre Sentís, 2019) Debemos considerar que en situaciones límite para la seguridad, incluso sin tener que llegar al extremo de una ciberguerra (Edgar: 425), se puede emplear una, llamémosla, ética alternativa (Edgar, 2003) (Himma & Tavani, 2008) (Clarke & Knake, 2010) que incluya el uso de la informática para el control de ciudadanos, pacíficos o no[3].

Durante años se ha utilizado el término legal de "Habeas Data" como un resumen de todo derecho sobre nuestros datos. Hablamos del derecho a conocer la existencia y acceder a los documentos que nos atañen, incluyendo datos genéticos, bancarios o cualquier fichero que conste en entidades públicas o privadas, del cual podremos conocer su uso, finalidad, origen y destino además de poder ejercer el derecho a la actualización de nuestros datos, su rectificación, limitación o anulación. (Latorre Sentís, 2019)

Las organizaciones, las empresas emplean bien las más de las veces la información de los ciudadanos, pero a veces se producen problemas. Los ejemplos posibles serían muchos: desde quien trafica con datos médicos que se almacenan en los hospitales a actividades poco honradas por parte de empresas que incluyen bombas lógicas en su software, de forma que si el número de registro no se ha introducido en una fecha determinada, el software, y quizá algo más, se borra (Barger, 2008). Esto, a caballo entre ética y ley a menudo se complica con episodios de falsedad documental, tales como la venta de títulos académicos online u otro tipo de documentación falsificada. Un ejemplo real puede ser el que (Girard, 2007): Un competidor puede hacer miles de clicks sobre los anuncios en Google de sus competidores para incrementar sus facturas. Aunque según Google no es sino un hecho aislado nos permite reflexionar.

Antes de dejar esta dimensión, vayamos a un caso extremo: los datos de los fallecidos, considerados desde el conocido derecho al olvido. El profesional tendría que establecer protocolos para borrar la presencia en internet de gente que ha muerto, evitar que extraños los insulten o se rían de ellos. Pero no todo se puede borrar, si hay referencias en diarios impresos quedan las hemerotecas y, por otra parte, es lógico que una parte de la información de individuos públicos sea preservada. (Latorre Sentís, 2019).

Derechos y obligaciones de propiedad:

¿Cómo se protegerán los derechos de propiedad intelectual tradicionales en una sociedad digital en la que es difícil rastrear y rendir cuentas sobre la propiedad, y es muy fácil ignorar dichos derechos de propiedad? Aquí podríamos plantearnos dilemas sobre los secretos comerciales, además de los clásicos relaticos a la propiedad intelectual, y la diferencia ente copyright y patentes. Eso si, consideremos que, en este caso concreto, hay diferencias significativas: distintos países, distintas leyes (Barger, 2008)

[3] Durante la legislatura de 1964 a 1968, el presidente de Estados Unidos Lyndon B. Johnson mantuvo unas tensas relaciones con J. Edgar Hoover, director del FBI. Este no dejaba de recurrir a escuchas telefónicas ilegales a fin de obtener información valiosa de otros dirigentes políticos, susceptibles de ser empleadas para coaccionarlos y chantajearlos. El presidente temiendo que acabase por intervenir su propio teléfono estuvo a punto de destituirlo pero desistió tras concluir con mordacidad "es preferible tenerlo dentro de la tienda meando para fuera, que fuera meando para dentro".

Partamos de un ejemplo que nos permite ver que en este caso no hay blancos y negros, no hay verdades absolutas, nos movemos sobre un paisaje gris. El 10 de octubre de 2007 el grupo Radiohead ofreció a sus seguidores la opción de pagar lo que quisieran por descargar su nuevo álbum "In rainbows". Si querían lo podían descargar gratis, o dar lo que quisieran. Alrededor de millón de fans lo hicieron el primer mes, de los que 6 de cada 10 no pagaron nada. Varios millones más se lo descargaron por P2P en lugar de hacerlo de forma gratuita desde la web del grupo. Fue el disco que más dinero le dio, sin tener que compartir el dinero con ningún sello discográfico. Cuatro meses después salió a la venta una versión de más calidad del álbum y llegó a ser el más vendido las listas americanas y británicas. En octubre de 2008 había vendido más de 3.000.000 de copias, de ellas 100.000 en una caja especial a un precio de 80 dólares y sobrepasaba las ventas de sus dos álbumes anteriores. (Porter, 2011)

Podemos pensar que internet lo ha revolucionado todo en este campo, pero, sin dejar de tener buena parte de certeza la afirmación, no lo es de forma completa. Antes de internet, existió la radio, y entre las dos, la televisión, que fue el modelo de medio de comunicación gratuito por excelencia. Un programa de una hora implica normalmente 48 minutos de programa y 12 minutos de anuncios con los que se paga el mismo. En 2009, por ejemplo, los anunciantes afirmaron haber pagado unos 230.000 dólares por un spot de 30 segundos en la serie de ABC Mujeres Desesperadas. A ese precio cada uno de los 10,6 millones de hogares que veía la serie tenía un valor para la cadena de 79 centavos. Y aparecen aquí los grabadores de vídeo digitales como el Tivo, que permiten a los telespectadores saltarse los anuncios, y por tanto amenazan con privar a las cadenas de su dinero al permitir que los seguidores de una serie la vean sin coste de dinero ni de tiempo[4]. Los ejecutivos planteaban que cada vez que un televidente se salta un anuncio está robando la programación, pero los telespectadores no tenemos obligación legal de ver nada, por mucho que se asuma un acuerdo económico implícito con el que se han sostenido las cadenas de televisión y que si fracasa, les forzará a encontrar otras fuentes de financiación[5]. (Porter, 2011) ¿Cuándo se vulnera de verdad la propiedad intelectual? ¿Es homologable el compartir una película en formato divx con un amigo, con la clásica copia de vinilo a cassette que el legislador en su momento previó? ¿Dónde trazar la barrera entre copia de seguridad y copia privada?

La vulneración de la propiedad intelectual la estudió desde el prisma ético (De George , 2003), creando la siguiente clasificación:

- Intercambio de películas, canciones… en los países desarrollados.

[4] Cuando el VCR llegó a los EEUU, la industria de la TV y el cine pusieron el grito en el cielo, con el argumento de que el VCR violaba las leyes de copyright. Los jueces dijeron que los VCR tenían muchos usos legítimos, uno de ellos el de grabar las emisiones para verlas de forma privada más tarde.
Se puede grabar un programa incluso si se vende comercialmente para verlo en otro momento, y también dejárselo a otro amigo, que interesado en verlo se equivocara a su vez al programar su vídeo. El principio para internet es, debería ser, el mismo (De George)

[5] Los problemas de los medios convencionales y sus ingresos no se deben a la difusión por los nuevos medios tanto como por las técnicas empleadas. En la prensa escrita, más antigua que la radio y la tv, el dinero viene no solo de la venta. De hecho el importe de compra es minoritario en los ingresos de las empresas: el dinero viene más de la publicidad que de la venta de periódicos. Cuando aparece la red, se pensó que se incrementarían los ingresos publicitarios reduciendo el coste de edición, pero esto no ocurrió. Y no por piratería ninguna, sino por una falta de adaptación a los nuevos modelos de negocio posibles. (Porter)

- Ingeniería inversa en determinados países, p.e. para copiar vacunas, retrovirales... el autor cita como ejemplo que China ha firmado todos los tratamientos internacionales sobre propiedad intelectual, pero dentro sus leyes parecen no tener efecto, planteándose ¿es malo salvar vidas usando un retroviral patentado, cuyo formulismo y forma de obtención ha sido "hackeado" de los ordenadores de una poderosa multinacional farmacéutica?
- Comprar menos licencias que copias instalan de un determinado software.
- Vender software que en principio no tenía precio, por ejemplo, creados con licencia creative commons. Y no solo software.
- Copiar programas para uso personal: el caso de un estadístico que se lleva a su casa para su uso y disfrute una copia de la última versión de SPSS disponible en su empresa. Sin pagar las licencias, evidentemente.

En lo que a nosotros respecta, hacemos una clasificación muy elemental: contenido y continente. El contenido para nosotros son los elementos que gracias a la informática pueden ser transferidos incluso sin conocimiento de los propietarios de sus derechos, y el continente, el software.

Al hablar de transferencia de contenidos lo que viene a la cabeza de muchos son las descargas directas y las redes P2P o Peer-to-Peer. Este tipo de protocolo se hizo famoso con Napster: los usuarios de forma gratuita, descargaban grabaciones en formato mp3. A resultas de esto, algunos músicos, productores, artistas y compañías presentaron demandas por infracción de derechos de autor contra Napster. Una anécdota poco conocida es que a medida que el asunto se complicaba en los tribunales, Napster comenzó a experimentar algunos problemas con su logotipo, que apareció en camisetas a la venta. Napster presentó una demanda contra los que utilizan la marca sin autorización, pidiendo daños y perjuicios. Posteriormente, Napster fue cerrado por un tribunal federal, y BMG lo compró. Otras plataformas aparecieron, como Grokster, Kazaa o Morpheus pero también fueron llevadas a pleito. La Asociación de la Industria de Grabación de América (RIAA) inició una agresiva política presentando demandas incluso contra los usuarios que descargaban canciones, intentando en los tribunales que los prestadores de servicios de Internet revelaran los nombres de los usuarios, a lo que algunas se resistieron (Jennings, 2009).

(Lessig, 2001) plantea un escenario terrible: en EE.UU, la industria creó un estándar para facilitar el control en la distribución de música. El congreso de EEUU a su vez, crea una ley que considera delito grave el crear SW que eluda tal control. Y una empresa que fabrica reproductores anuncia planes para cumplir esos estándares de control: el resultado es perverso: el control está codificado por el mercado, con el apoyo del estado.

Música, películas y… libros. Con la popularización de los libros digitales o e-books, se regresa al cultura vs propiedad intelectual. Es un viejo debate que lleva a reflexionar sobre la infraestructura de Internet y las herramientas digitales como bien común, no usándolas para satisfacer las necesidades de un modelo propietario y, esto es el eje del debate, que los derechos de autor no pueden imponerse a expensas de otros derechos fundamentales, y que solo un procedimiento judicial puede establecer sanciones (Aigrain, 2012). En este sentido, recordemos cuando se acusó a Google de despiadado por arramblar con su google books con

libros que, aun inencontrables en las tiendas y aun en las bibliotecas públicas, tenían sus derechos intelectuales. (Brandt, 2009) recuerda que el adjetivo de despiadado ya se aplicó en otra situación pasada: cuando la biblioteca de Alejandría se creó, gracias a los saqueos de los piratas ptolomaicos. Y no hace falta recordar cómo se nutrieron los principales museos de Londres (quizá gracias a lo cual, piedras miliares de nuestra cultura se han preservado hasta hoy)

Nos queda nuestro caballo principal de batalla. El software. (Bynum & Rogerson, 2004) PISWN UN reflexión sobre las diferencias entre patentes, secretos profesional o copyright, pero esto se nos queda corto, por ejemplo (Barger, 2008) se pregunta ¿Dónde encaja aquí, donde está el open software?, así que lo ampliamos con una visita al texto de Richard Stallman ¿Por qué el software debe ser libre? (Stallman, 2004)

Libre no es gratis, aunque tendemos a confundirlo. Por otra parte, lo gratuito no es exclusivo de internet. Pensemos en los regalos y su importante papel en muchas sociedades, como el potlach entre los nativos de la América noroccidental y el kula entre los melanesios de las islas Trobriand: ciclos de regalos virtuales que se dan entre las tribus vecinas. (Porter, 2011)

Tras las exposiciones anteriores, queda claro el posicionamiento que podamos mostrar a favor del software libre. Y es que, con Crespo, creemos que (Crespo Fajardo, 2012) el movimiento del software libre hace especial énfasis en los aspectos morales o éticos del software, viendo la excelencia técnica como un producto secundario priorizando su valor ético. El uso, la mejora y la distribución de herramientas libres y gratuitas permite revisar conceptos que hasta hace poco parecían inamovibles. La economía de mercado se convierte así en desarrollo sostenible y la comunidad de los desarrolladores es el núcleo de una verdadera y auténtica sociedad abierta, donde, además, se da por el efecto colaborativo una mayor calidad de las aplicaciones (Ippolita, 2010).

Es una idea que puede traspasarse, ojalá así fuera, al resto de las creaciones humanas: estamos acostumbrados a una visión dogmática de los derechos de autor. Es más, propugnar la idea de permitir a las personas que no son ni autores ni titulares de derechos de autor de una obra de arte, o una pieza de software, para compartirla con otras personas, equivale a la herejía (Aigrain, 2012).

Rendición de cuentas y control:

¿Quién puede y se hará responsable, además de rendir cuentas por el daño hecho a la información individual y colectiva, y a los derechos de propiedad? Hablaríamos de elementos como la rendición de cuentas a los individuos y a las instituciones. Y elementos de interés como el planteado aquí: si una persona se lesiona debido a una máquina controlada por software, ¿quién debe rendir cuentas de ello? (pensemos al respecto en los coches autónomos, o en un tablero de anuncios de ADIF o una pantalla en un centro comercial que transmita apología del terrorismo u algo ofensivo) ¿Hay un responsable? ¿o es lo mismo que con los proveedores de comunicaciones, como los teléfonos?. Se podrían analizar casos clásicos, como el robo por parte de hackers coreanos de datos de la seguridad social de EE.UU. o la sustracción del foro sobre enfermedades “Patients like me”.

Veamos este caso más despacio: PatientsLikeMe, pacientes como yo desde su origen: es un espacio que permite a una persona que sufre una enfermedad grave y busca en internet todo tipo de formación y apoyo emocional, encontrar un punto de reunión: una web, un foro, un espacio en una red social para compartir ideas, noticias o tratamientos, o cualquier otro tipo de información relevante sobre la enfermedad que sufre. Pero lo que no se previó fue proteger la información personal que figura en ese espacio y ésta termina llegando a una base de datos que es utilizada por la empresa que contrata… a ese paciente, a quien se le niega un posible ascenso por información recibida. (Latorre Sentís, 2019)

Otro ejemplo: la hegemonía de las grandes empresas sobre nuestros derechos. Pensemos que la Casa Real, distintos ministerios, aceptan sin pensar las TOS de Twitter y otras redes, que hacen olvidar el marco legal español para trasladarnos a Sillicon Valley. Por otra parte ¿va siendo hora de sembrar de denuncias a toda red social que se arrogue prerrogativas de juez? ¿Hasta dónde es lógico que se acorte la libertad de expresión? Los derechos fundamentales lo son, estés donde estés ¿podría una red social negar el acceso a gente según su raza o tendencia sexual? ¿No compiten las TOS, términos de servicio, con las leyes estatales? ¿Eso que dice Zuckerberg de "si (Facebbok) fuera un país, sería el país más grande del mundo", se supone que le posibilita situarse por encima de leyes nacionales e internacionales? Lo más importante ¿habría un juez que se atreviera a limitar sus actos?

Calidad del sistema:

¿Qué normas sobre la calidad de los datos y de los sistemas deben requerirse para proteger a los derechos individuales y la seguridad de la sociedad? El termino *calidad* redunda sobre el primer principio: si mantenemos un dato anticuado de un cliente, o bien si aún tan solo mantenemos el dato, cuando éste ha solicitado expresamente su deseo de ser dado de baja en nuestra base de datos, vulneramos la Ley.

Parece estrechamente relacionada con la anterior, pero es independiente de ella. Aquí nos preguntamos: ¿Cuál es un nivel factible y aceptable, desde un sentido tecnológico, de calidad de un sistema? ¿En qué punto se debe dejar de probar, y lanzar un software, un hardware? El marco legal puede dejar lagunas... ¿y si el usuario manipula nuestro producto? ¿deberíamos bloquear esa posibilidad? Lo difuso del asunto lo podemos ver considerando un sistema en el que hay errores solo predecibles y corregibles con un costo muy alto, tanto que no se podría comercializar ¿Y si no lo sacamos? ¿no llegaría hasta decaer la calidad de vida colectiva?. A este respecto, relacionamos las tres principales fuentes de un mal desempeño del sistema: a) bugs y errores de software; b) fallas de hardware o de las instalaciones provocadas por casusas naturales o de otro tipo y c)mala calidad de los datos de entrada.

Cuando pensamos en el culmen de la tecnología humana, a muchos lo primero que nos viene a la mente es la llegada del hombre a la luna (¡y de esto hace ya medio siglo!). Esta proeza fue posible gracias al uso de la informática por parte de la NASA. A priori, todo parece indicar que, si alguien debe usar siempre la última tecnología y estar pendiente de cualquier innovación, ha de ser la agencia espacial… pues no, lamento desilusionarles. Se supo que en el año 2002 la NASA adquiría en eBay un gran número de equipos médicos antiguos que contenían el microprocesador 8086 de la compañía Intel, el mismo que había empleado IBM para su ordenador personal en 1981. Un procesador varios millones de veces más lento y muchísimo

menos eficaz que los ordenadores de ese momento. La explicación es que el software que debía probar los motores principales de la lanzadera se había escrito en origen en ese procesador, el 8086 y si no podían ejecutarlo se acababan los lanzamientos. Y es que cuando los informáticos elaboran, limpian defectos y errores (vamos, se sumergen en un debug infinito) y ensayan con un software tan importe, están aterrados ante la idea de tener que modificarlo. El clásico "Si funciona, no lo toques. Si funcionaba, lo tocaste y ya no funciona, ¡tonto!". Pero no les faltaba razón: estos programas son tan complejos que nadie se atrevería a alterarlos y estar seguro de que funcionará la perfección en un aparato nuevo. La prueba de que la renovación es tan costosa, está en que ese mismo año la NASA dijo que iba a invertir 20.000.000 de dólares para actualizarlo.

Recapitulemos: la mayor hazaña tecnológica del ser humano, que supuso la conjunción de muchas ciencias y técnicas, apoyadas e impulsadas por la capacidad de cómputo, si, había avanzado… pero con un retraso de al menos dos décadas.

Calidad de vida:

¿Qué valores se deben preservar en una sociedad basada en la información y el conocimiento? ¿Qué instituciones debemos proteger para evitar que se violen sus derechos? ¿Qué valores y prácticas culturales apoya la tecnología de la información? Las tecnologías de la información pueden llegar a destruir elementos valiosos de nuestra cultura y sociedad, incluso aunque nos brinden beneficios. Si hay un balance de buenas y malas consecuencias ¿a quién responsabilizamos por las malas consecuencias?

Pensemos en la bomba atómica y su responsabilidad. No está en el avión que suelta la bomba ni tampoco en la bomba, sino en los científicos que concibieron el arma y en el coronel que escogió el momento para soltarla .La responsabilidad de nuestros actos no se transfiere a los objetos inanimados. Si esta decisión la toma un algoritmo, debemos intentar legar nuestra ética a las máquinas. (Latorre Sentís, 2019)

Habría muchos subtemas que encajar aquí, pero vamos a destacar uno que cada vez más implica a un mayor número de nuestros conciudadanos: los juegos, en concreto los juegos online.

Día a día, el número de personas que entran en la red, no en busca de unos minutos de charla, ni por buscar referencias de películas, canciones o libros, sino por jugar, por usar de juegos online, crece. Hay aplicaciones millonarias en usuarios, donde éstos pasan horas y horas.

¿No es tremenda ésta forma de perder el tiempo? (Lessig, 2001). Mientras el común de la población se dedica a trabajar sesenta, setenta semanales para empresas que no les pertenecerán jamás y creando futuros que no saben si llegaran a disfrutar, esas personas se dedican a diseñar y fabricar casas y construirse una vida allí, aunque sea virtual, trabajando a golpe de ratón, a falta de arado, plantando melones y cuidando cerdos virtuales que le permiten comunicarse con un nuevo código de relaciones con sus "cyberamigos" (Himma & Tavani, 2008) nos habla de los juegos, en concreto de los juegos compartidos, y de las relaciones que se generan, así como de la información que se comparte, así como de la realidad virtual y la simulación. Sobre juegos de más calado económico y la prevención de

riesgos, puede verse en (Cotino, 2008) "Juegos: prevención de riesgos y casinos de juego en internet".

Códigos éticos en relación con la informática

En el caso de la profesión informática, al margen de lo que los Colegios redacten en España, son ya clásicos los que proceden de las asociaciones profesionales toman el testigo y formulan sus códigos éticos. Los hay escuetos, como el del IEEE, o prolijos, como el de la ACM (Association of Computer Machinery).

Los códigos del Colegio profesional, de ACM y de IEEE son muy fáciles de localizar en internet. Búscalos.

También las empresas informáticas o asociaciones de ellas tienen sus propios códigos, y un estudio sobre su composición nos hace ver que en un elevado porcentaje, están centrados en la problemática de la protección de datos personales, que como vimos encajaba en una de las dimensiones morales. Pero hay más, como la particularización, referida por (Cotino, 2008), de Códigos de conducta en la contratación electrónica en España o la autorregulación para comunicaciones comerciales electrónicas.

¿Recuerdas la definición de código tipo? Relaciónala con la Protección de Datos. Pista: Acude al Reglamento Europeo de Protección de Datos y localiza referencias (directas o indirectas) sobre este asunto.

Mínimos a cubrir en cada dimensión moral por parte de un código ético de una empresa o asociación informática.

En este epígrafe seguimos de forma rigurosa a los profesores (Laudon & Laudon, 2016).

Normas éticas mínimas a incluir en atención a los derechos y obligaciones de la información:

- Privacidad del correo electrónico.
- Tratamiento de los datos de la empresa con respeto a las normas.
- Políticas de transparencia hacia los clientes.

Normas éticas mínimas a incluir en atención a los derechos de propiedad:

- Uso adecuado de las licencias de software.
- Respeto a la propiedad de instalaciones y datos de la empresa.
- Gestión adecuada de la propiedad del software creado por empleados de la empresa.
- Evitar ambigüedades en las relaciones contractuales con terceros.

Responsabilidad y control:

- Designación de un responsable único y bajo este, responsables de cada área (derechos individuales, derechos a la propiedad, derechos a calidad de sistemas, derechos a calidad de vida).
- Definición de responsabilidades de control, auditorías y administración.
- Detallar las responsabilidades legales de cada perfil laboral.

Calidad de los sistemas informáticos:

- Descripción de los niveles generales de calidad de los datos y el margen de error tolerable, con especificaciones detalladas para proyectos específicos.
- Exigencia de que todos los sistemas informáticos traten de estimar la calidad de los datos y las posibilidades de error en los sistemas.

Calidad de Vida:

- Establecer que el propósito de los sistemas es mejorar la calidad de vida de los clientes y los empleados al alcanzar altos niveles de calidad en los productos, en el servicio a los clientes, la satisfacción de los empleados, la ergonomía de los puestos de trabajo y usabilidad de aplicaciones, en el flujo de trabajo.
- Establecer un desarrollo adecuado de la gestión de los recursos humanos.
- Mantener de forma clara los límites entre familia, trabajo y ocio.

Una figura polémica. Hackers, hacking.

No es posible hablar de ética informática y olvidar esta figura que a nadie deja indiferente. Los medios de comunicación la ensalzan y ensucian, se odia y se ama. Se interpreta como algo bueno, y como algo malo, y esto viene de antiguo. De hecho, en el clásico de Stoll, *El huevo del cuco*, libro que dio pistoletazo a este tipo de cuestiones, podemos leer un párrafo que resulta clarificador en extremo (Stoll, 1990):

> *"Para Dennis el asunto del hacker era un problema de ética social.*
>
> *—Siempre habrá algunos cretinos metiendo las narices en nuestra información. Me preocupa que los hackers envenenen la confianza sobre la que se han construido nuestras redes. Después de muchos años intentando conectar un montón de ordenadores entre sí, un puñado de imbéciles pueden echarlo todo a rodar"*

Desde el principio, desde que alguien se consideró hacker, aparecieron sus propios códigos éticos. A veces escritos de forma rigurosa, otras como meros comentarios en grupos de news o foros, pero con puntos de partida que pueden seguir vigentes. Dudley los revisa desde 1984 y de él tomamos algunas claves (Dudley, Braman, & Vincenti, 2012) como que toda información debe ser libre y disponible para el público, incluido el derecho a acceder a los documentos confidenciales del gobierno. Tras revisar la situación una década más tarde, aparecen elementos que nos son conocidos por formar parte de cualquier código ético informático de hoy, tales como proteger la privacidad o ayudar a la seguridad, y otros elementos que nos pueden parecer de una actualidad tremenda hoy, como la necesidad de compartir, incluso procurando que los recursos de los equipos no se desperdicien. Aparece una serie de actividades prohibidas, que delimitan quien puede ser considerado un hacker y quien no: no se debe emplear software dañino, robar…

Lejos quedan ya aquellas reuniones de Black Hat, movidas por gurús de la informática de la época donde, a pesar del nombre, se trataba de reuniones de "sombrero blanco", o "ético", donde los hackers participantes eran personas que trabajaban (cuando no lo eran ellos mismos) para los directores de informática y jefes de seguridad informática de bancos y casi todo tipo imaginable de gran empresa (y muchas de tamaño mediano). Las empresas de software ya pensaban en ellas como en reuniones de chicos malos, pero aunque Bill Gates y Steve Jobs clamaran al cielo denunciando como ilegal la búsqueda y exposición de los defectos

de sus productos, no era un crimen. Lo sería si se utilizara el método desarrollado (el "exploit") para utilizar el defecto que ha descubierto en el software (la "vulnerabilidad") y emplearlo contra una red corporativa o el gobierno ("el blanco") (Clarke & Knake, 2010).

En este sentido conviene traer unas líneas de uno de los hackers más famosos de todos los tiempos, Mitnick (Mitnick & Simon, Ghost in the wires, 2011):

> *"Han pasado once años desde que salí de la cárcel. He organizado una consultoría que me proporciona un flujo constante de negocio. Me ha llevado a cada uno de los Estados Unidos y a todos los continentes excepto la Antártida. Mi trabajo hoy es, para mí, nada menos que un milagro. Intente buscar alguna actividad ilegal que, efectuada con permiso, pueda llevarse a cabo de forma legítima y beneficiar a todos. Solo una se me ocurrió: el hacking ético.*
>
> *Fui a la cárcel por el hacking. Ahora la gente me contrata para hacer las mismas cosas por las que fui a la cárcel, pero de una manera legal y beneficiosa. En los años transcurridos desde mi liberación, he sido orador principal en incontables eventos de la industria y las empresas, he escrito para la revista Harvard Business Review, y he sido profesor en la Facultad de Derecho de Harvard. Cada vez que algún hacker aparece en las noticias, me piden que comente la noticia en la Fox, CNN, u otros medios de comunicación. He aparecido en 60 Minutes, Good Morning America, y muchos, muchos otros programas. Incluso he sido contratado por agencias gubernamentales como la FAA, la Administración de la Seguridad Social, y a pesar de mi historial penal, en una organización del FBI, InfraGard."*

Confirmando el párrafo precedente, lo mismo que se mide como malo malísimo aparece después como algo que otorga valor. O, como decía el Marqués de Campoamor: "Nada es verdad, nada es mentira. Depende del color del cristal con el que se mira".

Esa misma doble moral la vemos en otro fragmento de otro libro de Mitnick (Mitnick & Simon, 2007) en el que valora la actuación de un hacker que, después de entrar en un sistema, avisa de las vulnerabilidades:

> *"En el caso de Adrián, el fiscal optó por no reparar en que las compañías supieron su vulnerabilidad a los ataques gracias a que el propio Adrián les informó de ello. En todos los casos, él ha protegido a las empresas informándoles de que sus sistemas tienen fallos de seguridad y esperando a que los hayan solventado para después permitir que las noticias de las intrusiones se publicaran. No cabe duda de que ha violado la ley, pero ha actuado (al menos en mi libro) con ética".*

Tipología

Establecer una tipología siempre es difícil. Quizá lo más efectivo, siguiendo a Joyanes (Joyanes Aguilar, 2010), sea hacer una clasificación atendiendo a su motivación, que puede pasar desde una mira alta, como buscar un cambio social o político, a metas como más prosaicas, como obtener un beneficio económico. El amplio abanico, de lo político o militar a satisfacer el propio ego quedan cubiertos. Otra posibilidad es atender a su objetivo: individuos, empresas, gobiernos, infraestructuras, sistemas y datos de tecnologías de la información; o el tipo de

estos últimos: públicos o privados. Por supuesto, queda reseñar el método que empleen: inyección de código dañino, uso de virus, gusanos, troyanos, etc.

Atendiendo a su autoría se podríamos hablar de (Joyanes Aguilar, 2010):

- Ataques patrocinados por estados, incluyendo casos de espionaje industrial; o desde los propios estados, como los perpetrados por los servicios de inteligencia y contrainteligencia.
- Efectuados por terroristas u extremistas político-ideológicos.
- Realizados por la delincuencia organizada, la mafia.
- Los más comunes: ataques de perfil bajo, realizados por personas con conocimientos variables.

En cuanto a la tipología de amenazas, también según Joyanes, encontramos una amplia batería, de la que destaca (Joyanes Aguilar, 2010):

- DDoS. (Distributed Denial of Service): Todo un clásico, que buscan hacer caer servicios como la web. Pueden realizarse utilizando redes de ordenadores previamente infectados por virus (botnet), que son cómplices involuntarios.
- Botnets: Redes de ordenadores zombis, usados para mandar spam, espiar datos bancarios… El número de ordenadores zombis en nuestro parque es, sencillamente, alarmante.
- Zeus: Hablábamos de los virus botnet (troyano). En concreto este recopila información del usuario, utilizándola para suplantar su identidad. Desde noviembre de 2010 se ha detectado su llegada a dispositivos móviles, inundando redes sociales.
- Otras amenazas futuras: Quedan abiertas dos áreas de impacto, una de las cuales, la ingeniería social, será visitada siquiera sea brevemente en este mismo tema, y, la otra, los ataques multivectoriales, una lógica evolución basada en la combinación de diferentes tipos de soporte como ataque: correo electrónico, mensajes en blogs, redes sociales…
- Stuxnet: Viene bien referenciarlo, pues nos sirve de previo a lo que denominaremos "ciberguerra". Se trata de un troyano que aprovecha una vulnerabilidad de los sistemas operativos Windows CC, empleados en los sistemas SCADA (Supervisory Control and Data Acquisition) utilizados en infraestructuras críticas tales como el control de oleoductos, plataformas petroleras, centrales eléctricas, centrales nucleares y otras instalaciones industriales con el objetivo de sabotearlos. Obviamente, no va orientado a ordenadores domésticos sino que está pensado para atacar a infraestructuras críticas o incluso sabotajes industriales. Una muestra de lo que desgraciadamente encontraremos.

Añadamos un factor. La informática avanza muy deprisa. En los años 90 un smartphone era un sueño de ciencia ficción. No hace mucho, la nube, el big data, o la inteligencia artificial como la conocemos ni siquiera hubieran sido consideradas por la ciencia ficción (un inciso: cuando leo a los clásicos de la ciencia ficción con mi e-reader, busco referencias de alguien que anticipara que alguien leería ese texto u otros con ese tipo de dispositivo… sin éxito). Y ya que hemos mencionado la nube… pensemos en una carpeta compartida en ella, por diez usuarios.

Si uno de ellos coloca una foto pederasta, todos los usuarios, en el momento en que la aplicación de escritorio actúe sincronizando con el disco local, estarán violando la ley. Este tipo de innovaciones disruptivas, como las llama Joyanes (Joyanes Aguilar, 2010), tienen un fuerte impacto en la seguridad. También termina reseñando como elementos de riesgo la realidad aumentada y la Internet de las cosas.

> Cabe hacer un recordatorio en estos momentos: las figuras y términos que en este tema se emplean tiene, es obvio, un prisma ético y deontológico, pero también uno marcadamente legal, con dos referencias ineludibles: el Código Penal y el Esquema Nacional de Seguridad.

Por no dejar de traer a colación el llamado hacking ético, y siguiendo a Himanen (Himanen, 2004), podemos considerar por encima de la ética hacker que lo relaciona al trabajo y al dinero a la llamada *nética* o ética de la red. Con esta expresión aludimos a la relación que el hacker mantiene con las redes de nuestra actual sociedad. Se trata un término a no confundir con el habitual de *netiqueta* (que incluye principios de conducta tales como "evitar expresiones inadecuadas", "no usar mayúsculas", etc.). Esta relación del hacker con las redes de comunicación de nuestra sociedad se remonta al origen de la ética hacker, en la década de 1960, la nética, pero recibió un fuerte impulso en 1990 cuando se reformuló a través de la Electronic Frontier Foundation, por Mitch Kapor (creador de la hoja de cálculo Lotus) y John Perry Barlow, desde donde se intentó potenciar los derechos del ciberespacio.

Elementos de interés

A modo de cajón de sastre, hay dos elementos que no podemos dejar de tratar aquí: la llamada ingeniería social y la últimamente tan de moda "ciberguerra".

Ingeniería social

Abrimos el epígrafe con una referencia de Mitnick que nos servirá para ahondar no solo en la doble moral que parece traslucirse…, sino en la duda de si es mejor o peor engañar a máquinas, o a seres humanos: (Mitnick & Simon, 2007)

> *"Mientras Mudge únicamente utilizó métodos técnicos en el ataque que nos ha descrito, Dustin utilizó también la ingeniería social. Aunque él no se siente muy cómodo por eso. No tiene ningún reparo en los aspectos técnicos del trabajo y admite disfrutar cada momento de un proyecto. Pero cuando tiene que engañar a la gente, cara a cara, se siente violento.*
>
> *He intentado analizar por qué es así. ¿Por qué un método me descompone y el otro no me afecta en absoluto? Quizás nos han educado para no mentir a la gente, pero no nos han enseñado ética informática. Estoy de acuerdo en que, por lo general, tenemos menos reparos en engañar a una máquina que en engañar a otra persona.*
>
> *Aun así, a pesar de las dudas, normalmente siente la carga de adrenalina siempre que supera un episodio de ingeniería social que discurre sin problemas".*

La idea básica que sustenta la ingeniería social es la siguiente: en muchos casos, es más fácil y eficaz engañar a las víctimas para que nos den la información que queremos que robársela. El engaño que se produce es psicológico, más que tecnológico, precisando habilidades en áreas como la psicología y la lingüística que combinan con sus conocimientos de informática (Kshetri,

2010). Es el hombre el eslabón más débil de la cadena que representan las tecnologías de la información, y por tanto el más susceptible a partirse. El ingeniero social lo toma de blanco y esto provoca reacciones enfrentadas. Desde el campo de la psicología, Mitnick (Mitnick & Simon, 2007) nos trae una cita del Dr. Brad Sagarin, psicólogo social, que dice: "El ingeniero social emplea las mismas técnicas de persuasión que utilizamos todos los demás a diario. Adquirimos normas. Intentamos ganar credibilidad. Exigimos obligaciones recíprocas. Pero el ingeniero social aplica estas técnicas de una manera manipuladora, engañosa y muy poco ética, a menudo con efectos devastadores."

Hay múltiples maneras de conseguir esos fines. (Hadnagy, 2011) nos habla, por ejemplo, de la reciprocidad. Se trata de algo inherente a la expectativa que todos tenemos de ser bien tratados cuando somos amables con los demás. Esto, es más importante de lo que parece pues a menudo el favor se devuelve inconscientemente. Otro factor importante, también según Hadnagy, serían los incentivos ideológicos. Cada persona tiene unos ideales y creencias[6] diferentes a los de los demás, y estos afectan a esa definición. Si el sueño de tu vida es dirigir una empresa de informática orientada a la gestión, entonces esa es tu pasión, que provocará que trabajes más horas y más duro que cualquier otro empleado, y posiblemente lo hagas por menos dinero, ya que es tu motivación, mientras que para los demás es solo un trabajo del que salir cuanto antes. Las horas extras mal cobradas te pesarán menos. Sabrás que te explotan, pero te dolerá menos.

Dado que la gente es pues arcilla moldeable, como hemos visto, comprenderemos que la tarea del ingeniero social se puede hacer más fácil o más difícil. Fácil, pues amasa una arcilla ya ablandada, o difícil, si intenta remar a contra corriente.

[6] Los sueños y las creencias pueden ser algo tan arraigado en una persona que separarlo de esa persona puede ser casi imposible. Cuando se escucha la frase: "Yo tengo un sueño ", la mente nos lleva a pensar en Martin Luther King, así como cuando oímos "No tengáis miedo", pensamos en Juan Pablo II. Alrededor de estos nuevos tótems humanos se configuran grupos relativamente próximos en pensamiento, donde se mueven personas con tendencias similares. La gente tiende a ser atraída a otras personas con sueños y objetivos parecidos, "Dios los cría y ellos se juntan", que dice el refranero, pero también es un factor que los convierte en fácilmente manipulables. Y a veces no es necesario que exista ese tótem o nexo de unión, pues se puede fabricar. Así, el dominio que la casta política posee de los medios de comunicación en un camino acelerado a la neolengua de Orwell en su tristemente profético 1984, convierten a la gran masa en un grupo de personas con pensamiento plano. Personas que tienen ideas afines, las más de las veces generadas a través de un refinado lavado de cerebro que se ejecuta de forma invisible, van haciendo más grande el factor de iniciación a esta nueva marea humana: la espiral del silencio crece, de tal manera que cuando alguien sabe en su fuero interno que lo que le rodea está equivocado, no habla, para no ser señalado como el malo de la película, o, usando el vocabulario de nuevo cuño, el "terrorista" o "el fascista", y termina siendo uno más confundido en la masa. Unas pocas consignas, o discursos emotivos, podrán enardecer o hacer derramar lágrimas al conjunto de personas de forma que participen sin dolor regalando parte de su dinero duramente ganado. Sus ideales han sido cambiados, manipulados, sin recurrir a lo que en otros momentos históricos era la herramienta común: el miedo. Aunque hay que reconocer que no son una novedad: en la educación, por ejemplo, se ha usado desde hace siglos para enseñar a los niños a través de cuentos y fábulas con un significado oculto o moraleja: Hans Christian Andersen o Los Hermanos Grimm son excelentes ejemplos. Hoy podemos ver guiños en la comercialización, donde se usan anuncios "afines a nuestros ideales": recordemos la campaña de Ikea que, en un momento en que la monarquía tenía una tasa de popularidad baja, usó como lema "la república independiente de mi casa".

Para cerrar el apartado, cabe destacar una actividad profesional nueva que surge al respecto de la existencia de la ingeniería social: la auditoría de ingeniería social. Se trataría de aquella situación donde un profesional es contratado para poner a prueba a las personas, las políticas, y el perímetro físico de una empresa mediante la simulación de los mismos ataques que un ingeniero social malicioso usaría. Las dos principales diferencias entre un ingeniero social malicioso y un auditor profesional son las siguientes: el auditor profesional siempre tratará de ayudar y no avergonzar, robar o dañar a un cliente, y, esta es la que más nos interesa a nosotros, un auditor profesional seguirá las pautas morales y legales existentes (Hadnagy, 2011) (Mitnick & Vamosi, 2018)

Ciberguerra

Hablemos ahora aunque brevemente de un fenómeno a medio camino entre el hack y la seguridad del estado, la ciberguerra. Desde el ministerio de Defensa de España, Joyanes recuerda algo que nosotros ya conocemos por Clarke: (Joyanes Aguilar, 2010) (Clarke & Knake, 2010): Richard Clarke prevé o se imagina un fallo catastrófico "en cuestión" de quince minutos. Se imagina que los errores de los ordenadores llevarán a la caída de los sistemas de correo electrónico militar; las refinerías y los oleoductos explotarán, los sistemas de control de tráfico aéreo se colapsarán; los trenes de pasajeros y de carga y los metros descarrilarán; las redes eléctricas de los Estados Unidos se caerán; las órbitas de los satélites quedarán fuera de control. Y lo que es peor de todo, la identidad del atacante puede ser un misterio.

Esta situación que pinta Clarke, en un escenario catastrófico que enfrente a EE.UU y China, no está tan desencaminada. Los servicios secretos de EE.UU. hace tiempo que divulgaron la existencia de manuales de "guerra irrestricta" definiendo como debían actuar sus informáticos especializados al respecto.

Estamos hablando de ataques dirigidos desde arriba, aunque no hay que descontar la ayuda de "espontáneos", como señala (Libicki, 2009) los ataques pueden provenir de terceros, lo que generará más confusión todavía. Esto suele ocurrir cuando la tensión entre dos estados se deja ver a la sociedad en general, como pasó, recordemos, con el suceso de la isla Perejil entre Marruecos y España. Esto legitimaría éticamente los ataques de los hackers que se sintieran más o menos patrióticamente insuflados por los vientos de guerra.

Un matiz intermedio es la cyberdisuasión (Libicki, 2009), que se trata de un estadio anterior, donde amagar la mano sin llegar a tirar la piedra. Asustar. Con la ciberguerra un estado podría atacar, sufrirá represalias, y vivirá para atacar a otro día, con la disuasión intentaríamos que no llegase a atacar. También es simétrica, ya que se lleva a cabo entre iguales. Desde un punto de vista moral, el que toma represalias no está a priori a un nivel moral más alto que el otro. No hay que pensar que el objetivo último es ganar (p.e. en un conflicto nuclear), sino la propia disuasión. Para dejar claras las diferencias entre ciberguerra y ciberdisuasión, vemos la tabla siguiente, basada en (Libicki, 2009)

Tabla 6 Diferencia entre ciberguerra y ciberdisuasión. Adaptado de Libicki.

Pregunta	**Ciberdisuasión**	**Ciberguerra**
¿Quién lo hizo?	No se puede saber sobre quién	El objetivo ha sido ya seleccionado

	ejercer represalias en su contra.	por otras razones.
¿Nos pone en riesgo?	No se sabe. El efecto deseado es impedirlo.	Es importante saberlo, pero no crítico, para justificar y dar forma a un mayor esfuerzo.
¿Se produce varias veces?	No se puede saber si la represalia es repetible.	Afectará la intensidad del esfuerzo a través del tiempo.
¿Intervienen terceros?	Pueden interferir en los "avisos".	Pueden incrementar la gestión de la escalada de tensión.
¿Hacemos llegar el mensaje correcto?	La política de disuasión puede crear un riesgo moral.	La carga moral ya ha sido aceptada.
¿Existe un umbral a no traspasar?	Puede interferir en el desarrollo.	Los umbrales más importantes ya se han traspasado.
¿Evitamos la tensión?	Haciéndolo reducimos la credibilidad de las represalias.	La ciberguerra es ya más que la intensificación de la tensión.
¿Vale la pena "golpear"?	La represalia puede ser fútil.	Sí, si podemos cubrir una serie de objetivos.

Trastornos y enfermedades derivadas de las TIC

Las TIC no solo pueden estudiarse desde el prisma de lo que sucede con los actos del trabajador, y cómo éstos pueden afectar a su trabajo o a los demás, y no debemos olvidar que puede tratarse el caso inverso: como el trabajo puede afectar al trabajador, bien físicamente o psíquicamente (Edgar, 2003) mediante elementos como el tecnoestrés y las llamadas "tecnodolencias" (*technomalady*: problemas musculares, dolor de ojos, vómitos...

Son de sobra conocidos los riesgos para la salud, tanto por el agravamiento de problemas existentes como por la aparición de nuevos. Pongamos por ejemplo las lesiones por esfuerzo repetitivo (el tipo más común relacionado con el uso de ordenadores es el síndrome de túnel carpiano) o el síndrome de visión de computadora (CVS): cualquier condición de fatiga ocular relacionada con el uso de las pantallas.

De entre las desconocidas hasta la aparición de las TIC en la vida cotidiana destacan el Tinnitus (el escuchar zumbidos, oír timbres fantasma de móvil, notificaciones que no existen), la nomofobia (el miedo a salir a la calle sin teléfono) o el tecnoestrés: estrés inducido por el uso de ordenadores, por ejemplo por llegar a esperar que las otras personas e instituciones humanas se comporten como computadoras, den respuestas instantáneas, estén atentos y demuestren una falta de emoción. Otros síndromes relacionados serían el de la ignorancia (la informática es una caja negra, se sabe lo que se hace pero no cómo se hace), el de la complejidad (es un mundo tan complicado que es imposible entrar a explicárselo y mucho

menos poner normas) o el de realidad virtual (como lo que hay en internet no existe ¿para qué preocuparnos de ello?)

El miedo al cambio no debe tampoco ser desdeñado. Tenemos una visión, quizá más heredada de las películas que de la realidad, del gran inventor que de golpe lo revoluciona todo, generando con su portentoso cerebro inventos dignos de los inquilinos del Olimpo. Sobre esto se ha discutido mucho, ya en "la evolución de la tecnología" George Basalla rechazaba esa visión apostando en cambio por la concepción darwiniana del cambio gradual. Basalla documenta que la aparición de los inventos célebres (de entre los que destacaremos entre otros el transistor y la máquina de vapor) no son más que el resultado de numerosos cambios sucesivos menores o, mejor, de la combinación de pequeños elementos ya existentes. Quizá una pedagogía basada en estos presupuestos sería suficiente para combatir esa resistencia que se presenta en forma de miedo al cambio.

Otra categoría podría enfocarse en torno a las patologías sexuales. En este asunto, seguimos a (Smoller, 2014) de forma íntegra. Jordan Smoller se plantea sobre la idea de que internet ha provocado un aumento de la pedofilia sobre si ésta y otras parafilias son muy comunes. Y se responde que realmente no lo sabemos. Si vamos puerta a puerta preguntando si le atraen, digamos, los niños de 8 años, nadie lo va a reconocer. De hecho no lo dicen hasta que son detenidos, e incluso después lo siguen negando. Smoller cree imposible realizar un estudio epidemiológico al respecto, pero donde sí se manifiesta es en torno a otra expresión sexual en internet: el fetichismo. Internet está repleta de webs con redes sociales de fetichistas. Cita un estudio para intentar averiguar cuál es el fetiche más común, empleando Yahoo para rastrear Internet en busca de grupos de debate relacionadas con el fetichismo, que dio como resultado 400 grupos con miles de miembros cada uno, y tras clasificarlos se encontró un claro ganador: los fetiches relacionados con los pies pulverizan a la competencia y suman un 47% de los fetiches relacionados con el cuerpo seguidos por un 9 % relativos a los fluidos corporales. En el caso los objetos inanimados, casi un tercio de esos grupos hablaban de zapatos.

Smoller sigue avanzando con una reflexión objetiva: en los últimos años del siglo pasado se produjo un hecho que condujo a un cambio sin precedentes en la experiencia sexual humana: por primera vez en la historia millones de personas podían ver a otras realizando el acto sexual. Había llegado internet. Pero esto no es un cambio radical, una aportación nueva al humano, pues el auge de la pornografía en Internet no es más que el último capítulo de la historia entrelazada de la tecnología y el estímulo sexual. Da como ejemplo la llamada escatología telefónica (llamadas telefónicas sexuales). Aquí hay un trastorno psiquiátrico que solo fue posible con la invención del teléfono. Con el avance de la tecnología de la comunicación el teléfono ha quedado desfasado, y existen indicios de que la escatología telefónica se va haciendo menos común, pues existen otros medios para ocupar su lugar (los mensajes eróticos, el llamado sexting).

Como se anticipaba, no resulta algo nuevo. Smoller insiste en que la historia de la evolución conjunta de la conducta sexual y la tecnología se remonta a mucho antes. La invención de la imprenta en el siglo XV permitió la difusión de libros y folletos obscenos. En el siglo XIX llegó la fotografía, que inundó el mundo de un nuevo tipo de imaginería sexual, y por supuesto en el siglo XX el cine la televisión y el vídeo familiar crearon toda una industria de la pornografía que

entro en nuestras casas. Aunque reconoce que por su descomunal alcance volumen y variedad la web no tiene parangón como medio de difusión de la pornografía.

De la robótica a la Inteligencia Artificial ¿un cambio de ética?

Dudley (Dudley, Braman, & Vincenti, 2012) plantea que dada la dificultad para los usuarios medios, el hombre de la calle, al interpretar las leyes, se abren dos posibilidades para el legislador: una, crear leyes de fácil lectura y sin ambigüedades para que sean fácilmente comprensibles por todos los usuarios del ciberespacio, y otra codificar la propia ley en los programas de ordenador de forma que los usuarios queden protegidos. Una derivad extrema, que ya se aplica, como pronto veremos, es que la justicia se ejerza mediante máquinas dotadas de inteligencia artificial que puedan sustituir al juez.

Lo cierto es que los documentos legales, por simples que sean, pueden no llegar a leerse nunca. Pensemos en cuántos de nosotros leemos unas simples condiciones de servicio, las TOS. Lo que nos lleva a valorar la segunda parte: la informatización de las leyes. El principio fundamental sería evitar daños a los usuarios, lo que dentro de la ética en general nos lleva a la ética de la máquina en concreto.

La ética de la máquina definiría, siempre según Dudley, cómo deben comportarse las máquinas con los usuarios humanos y con otras máquinas, haciendo énfasis en evitar el daño y otras consecuencias negativas de las máquinas autónomas o programas de ordenador sin control. El estudio de esta parte de la ética cada vez tiene más eco en el seno de la UE, como lo muestra la Declaración sobre Inteligencia artificial, robótica y sistemas "autónomos" (Comisión Europea. Grupo Europeo sobre Ética de la Ciencia y las Nuevas Tecnologías, 2018) y otros interesantes documentos fácilmente localizables mediante EURLEX (EUR-Lex, 2019).

De base se parte de la idea de que para construir máquinas éticas, debemos antes entender cómo los seres humanos emplean la ética en la toma de decisiones, y luego tratar de traspasar estas conductas a las máquinas. Como todo, arrastra ventajas e inconvenientes. Como ventajas obvias, al tratarse de máquinas que no necesitan comer o dormir, contaríamos con su permanente disponibilidad y por supuesto con su "fría" impasibilidad. Además su gran capacidad de trabajo nos proporcionaría, para el caso de tener que valorar distintos supuestos en dilemas éticos, una gran capacidad para simulaciones y la no existencia de límites sobre el número de casos evaluados. Por el contrario, aparecen problemas, pues crear nuevos conjuntos de reglas específicas, o adaptar las existentes a los casos que se presenten, genera un cuello de botella que es muy conocido en los sistemas de inteligencia artificial. Además, es necesario determinar los puntos claves de la ética y leyes que están siendo incorporados dentro de un sistema y ¿quién vigila a ese vigilante? (Dudley, Braman, & Vincenti, 2012). De ahí que la UE busque la construcción de un marco ético y legal común e internacionalmente reconocido para el diseño, producción, uso y gobernanza de la inteligencia artificial, la robótica y los sistemas "autónomos". (Comisión Europea. Grupo Europeo sobre Ética de la Ciencia y las Nuevas Tecnologías, 2018)

Los elementos que preocupan son muchos y diversos, desde los automóviles que no necesitan de un conductor, los drones autónomos, robots exploradores, bots financieros, y el diagnóstico médico asistido por aprendizaje profundo (*Deep Learning*), así como la inteligencia artificial (IA) en la forma de aprendizaje automático (*Machine Learning*), la mecatrónica avanzada (una

combinación de IA, aprendizaje profundo, ciencia de datos, tecnología de sensores, internet de las cosas y las ingenierías mecánica y eléctrica), el incremento de la interacción entre los humanos y las máquinas (como en el caso de los interfaces cerebro- computadora y los ciborgs) y el Big Data, entre otros. De esto deriva la preocupación de la UE (Comisión Europea. Grupo Europeo sobre Ética de la Ciencia y las Nuevas Tecnologías, 2018), por las consecuencias como la redefinición el concepto de trabajo, la mejora de las condiciones de trabajo, y la reducción del aporte y la interferencia humana durante las operaciones.

Profesionales e IA.

El test de Turing, primero llamado juego de la imitación fue publicado en "Computing Machinery and intelligence", 1950 (Latorre Sentís, 2019). Durante décadas ha sido el elemento clave para poder verificar si una IA era similar a la humana. Con esta imagen tan gráfica en la cabeza, tendemos a olvidar que Turing, que los programadores, que los creadores de las IA, son humanos, y no solo humanos, sino profesionales de la informática y ciencias relacionadas.

Los programas que originan el embrión están escritos por programadores, con un trabajo que no es sencillo. Latorre subraya que para muchos empresarios este trabajo no es relevante, lo que es un error grave. Que un sistema informático funcione, a día de hoy, depende de la buena preparación de la persona que lo establece y gestione. Si fuéramos a tomar un avión donde supiéramos que el piloto tiene tendencias suicidas, nos lo pensaríamos. De forma similar, debemos con respecto al programador comprender en todo lo posible su forma de pensar y proceder. (Latorre Sentís, 2019)

Pero detengámonos en este punto, y pongamos acento en algo que acabamos de decir: los programas que originan el embrión de la IA. Porque hoy por hoy, estos sistemas ya se retroalimentan y mejoran solos, dando al tiempo más capacidad pero también más opacidad, al no saber exactamente que hacen las nuevas líneas de código. Frecuentemente se decía: "jamás existirá una máquina que sea capaz de hacer tal o cual cosa"; "una máquina nunca sabrá más que su constructor"; "siempre será necesario un hombre para conducir vigilar o reparar la máquina". De todas las proposiciones, esta es la más falsa de todas. (David, 1973)

A este respecto pensemos en algunos ejemplos que nos da la propia (Comisión Europea. Grupo Europeo sobre Ética de la Ciencia y las Nuevas Tecnologías, 2018): Google Brain desarrolla una IA que al parecer construye otras de su misma naturaleza mejor y más rápidamente que los humanos. Pensemos también en AlphaZero y el ajedrez o AlphaGo y el Go, que explican como pocos elementos que es eso del aprendizaje profundo y los llamados "enfoques de redes generativas antagónicas" (*generative adversarial networks*), máquinas que se "enseñan" a sí mismas nuevas estrategias y adquieren nuevos elementos para ser incorporados en sus análisis. Esto, como hemos anticipado, y que resulta algo que causa preocupación a la Comisión Europea, provoca que las acciones de estas máquinas se vuelvan indescifrables y escapen del escrutinio humano, tanto porque es imposible averiguar cómo se generan los resultados más allá de los algoritmos iniciales, como porque el rendimiento de estas máquinas se basa en los datos utilizados durante el proceso de aprendizaje y estos pueden no estar disponibles o ser inaccesibles. Pero aún hay más: si estos sistemas usan datos con sesgos y errores, es muy difícil volver atrás.

Toma de decisiones por la IA

Hay decisiones que tomamos los humanos y que causan rechazo en general al considerar que puedan ser tomadas por las máquinas. Por llevarlo a la esfera más alta, el gobierno de las naciones. Hemos visto cómo se reparten los poderes dentro de un estado: los parlamentos legislan, los gobiernos (poder ejecutivo) ejecutan las leyes y los jueces supervisan su cumplimiento. ¿Y si alguna de esas cosas lo hiciera una inteligencia artificial? Aparecen voces diciendo que no solo podríamos hacerlo, sino que deberíamos, para obtener las mismas ventajas que ya se reciben, o al menos se atisba por su proximidad, en la asistencia a operaciones médicas, la conducción de vehículos o generación de nuevas medicinas, con un factor que hace más deseable su aplicación: erradicar la corrupción y eliminar las influencias no justificables de lobbies. (Latorre Sentís, 2019)[7]

En el caso de los jueces los primeros pasos ya se han dado. En Estados Unidos se emplea IA para ayudar a establecer fianzas o estimar el riesgo de ciertas decisiones judiciales. El software empleado recibe el nombre de "*Public Safety assessment*", evaluación de riesgo público. Es obvio que el sistema anglosajón basado en la jurisprudencia es un buen candidato ser empleado de forma eficiente por inteligencias artificiales. (Latorre Sentís, 2019)

Pero nos queda plantearnos el cogollo de la cuestión: más allá de que ética programar… ¿Quién la decide? Y aún más ¿Quién escribe esas subrutinas?

Vamos a ver la importancia de esto con un ejemplo. Imaginemos a dos trabajadores de un hospital que escriben un programa para que suministre datos a la inteligencia artificial que analiza las imágenes de la resonancia magnética y determina la localización de determinados tipos de tumor. Pepe y Paquita, que así se llaman nuestros sujetos de estudio, tienen abierto un litigio contra el hospital por impago de horas extras, sí que a Pepe se le ocurre que puede esconder en el código una subrutina que le permita alterar los datos desde cualquier terminal de consulta del hospital, mediante una pulsación determinada de teclas. Esos datos alterados forzará un 15% de diagnósticos incorrectos, una cantidad suficientemente baja para no ser detectada enseguida. El hospital termina enfrentándose legalmente con ellos y, tras un juicio que le es favorable, los despide. Pepe pone en marcha su código. En un año, diez pacientes fallecen por un diagnóstico equivocado. ¿Cómo era la ética de Pepe? Realmente de un perfil muy bajo, pues despreció la vida humana. Pero ¿alguien debería haber supervisado el código? ¿Paquita pudo ver algo y callar? Todo responsable debe ser identificable, así que la respuesta a la primera pregunta es obvia: sí. Todo código debe ser revisado y, en la medida de lo posible, los algoritmos deben operar con un código público, visible. La idea del código abierto parece chocar con los intereses comerciales, pero hay que encontrar un equilibrio. Al menos para poder seguir la trazabilidad y, por supuesto, si hablamos de inteligencias artificiales que se corrigen solas. (Barrio Andrés, 2018)

Pero no hace falta pensar tan solo en decisiones de alto impacto. También se afecta nuestro día a día. Hay múltiples evidencias de una inevitable emancipación de las máquinas frente al

[7] Hay una serie de consideraciones sobre la condición inherentemente política de la tecnología que nos hace (Colmenarejo Fernández, 2017):

- Las innovaciones tecnológicas lejos de ser neutrales siempre están orientadas a un fin político.
- Las tecnologías se ven afectadas por y desde lo social y no como un factor independiente.

humano, sin ir más lejos, el uso de Google[8], Facebook o Spotify que se han emancipado ya de la memoria humana, sometiéndola y que pueden llegar a conformar nuestra propia identidad, de acuerdo a parámetros que no elegimos nosotros. Consideremos algoritmos que eligen por nosotros contenidos de nuestra biografía y que parecen saber más de nosotros que nosotros mismos, no sólo en nuestro pasado si no y aquí más probablemente, de los nuestros deseos futuros. Y no solo hablamos de memoria: las máquinas se han emancipado ya de la intuición humana. Pensemos en la diferencia que podemos comprobar entre dar un paseo guiados por Google Maps o dejar tan solo que la ruta acabe tan lejos como los pies nos lleven. Memoria, intuición ¿Queda algo por someter? Pues sí, nuestros sentidos, que sucumben ante el hechizo de las gafas de realidad virtual o videojuegos con realidad aumentada. (Colmenarejo Fernández, 2017)

Sistemas autónomos

Desde una perspectiva ética, es importante tener en cuenta que (Comisión Europea. Grupo Europeo sobre Ética de la Ciencia y las Nuevas Tecnologías, 2018) la autonomía solo puede ser atribuida a los seres humanos, pero el empleo extensivo del término tanto entre el público en general como entre la comunidad científica en particular para hacer referencia al grado más alto de automatización y de independencia de los seres humanos en términos de "autonomía" operativa y de toma de decisiones provoca que tendamos a olvidar esa única atribución posible. Pero, para nuestro estudio, ya que un sistema inteligente no pueda ser considerado "autónomo" en el sentido ético, nos indica que tampoco puede ser considerado titular de la moralidad y dignidad humanas. Esto por su parte, implica que los humanos tenemos que seguir manteniendo el control en aquellos ámbitos que conciernen a los seres humanos y su entorno y así poder seguir decidiendo en (Comisión Europea. Grupo Europeo sobre Ética de la Ciencia y las Nuevas Tecnologías, 2018) cuestiones tan importantes como los valores que fundamentan la tecnología, aquello que debe ser considerado moralmente relevante, y los objetivos últimos y los conceptos de lo que es bueno.

Las preocupaciones de la UE en este sentido se centran en tres elementos principales.

1. Los sistemas de armas "autónomos".
2. El software "autónomo", los bots. Hoy ya manejados en el comercio y las finanzas, además de por aquellos sistemas inteligentes actuales mantienen diálogos con clientes en centros de atención telefónica. La Comisión Europea plantea un tema más allá de la privacidad, y es si tenemos a saber si hablamos con un ser humano o con una IA[9].

[8] Sobre el botón de apagado de Google cabe incluir una reflexión de Latorre, que es muy acertada: Todos los peligros inventados en la ciencia ficción pueden ser irrelevantes. Por el contrario, no somos capaces de comprender que terribles consecuencias tendría una irrupción abrupta de la inteligencia artificial avanzada. En este sentido, Google ya ha establecido un botón de apagado de todos los algoritmos avanzados que utiliza. Está en las manos de esta empresa cortar el enorme flujo de procesamiento de información que nos asiste. Creo que da tanto miedo al descontrol de la inteligencia artificial cómo dejar de tenerla. ¿Viviríamos en una gran ciudad sin agua, sin electricidad, sin coches? Durante el gran apagón de 1977, la ciudad de Nueva York se convirtió en un caos, donde las más bajas pasiones humanas se desataron. Habría que evitar usar el botón de apagado de la inteligencia artificial avanzada, por nuestro bien.

[9] Muy relacionado, y también estudiado por Dudley, está la ética del juego. El juego aquí considerado como elemento lúdico donde se apuesta algo de valor, con conciencia del riesgo y esperanza de ganar, sobre el resultado de un concurso, o un acontecimiento incierto cuyo resultado puede ser determinado

3. De forma más amplia en los espacios de opinión pública, aparecen los vehículos que no necesitan de un conductor, aunque de momento el debate parece centrarse en casos excepcionales, usualmente llamados "dilemas del tranvía"[10]. Como indica la Comisión Europea, esta interpretación suscita un enfoque calculador, que generalmente aplica parámetros excesivamente simplistas a las realidades humanas, lo que por otra parte provoca que ignoremos preguntas de más calado como "¿qué decisiones relativas al diseño se tomaron en el pasado que condujeron a este dilema moral?", "¿qué valores deben contribuir al diseño?", "¿cómo se deben sopesar estos valores en caso de conflicto y quién debe sopesarlos?", "¿qué indican los abundantes datos empíricos que se están acumulando sobre la forma en la que las personas deciden en los casos del dilema del tranvía y cómo se traducen esos resultados a las configuraciones automáticas para vehículos?". (Comisión Europea. Grupo Europeo sobre Ética de la Ciencia y las Nuevas Tecnologías, 2018). En un plazo breve o medio, pueden haber pocos o muchos accidentes de coches autónomos, pero será un hecho que los coches serán controlados por máquinas. Tampoco importa si estamos de acuerdo o no, o si creemos que es más o menos viable económicamente. A principio del siglo XX, cuando los vehículos primero eléctricos y luego con motor de explosión empezaron a recorrer nuestras ciudades, se generó un movimiento de protesta, que alegaban que habrían muchos muertos. Y es cierto, en un solo día los muertos por accidentes de tráfico superan los muertos durante décadas por accidentes con caballos o carretas de bueyes pero… ¿Cuántos caballos o carretas de bueyes circulaban hoy por nuestras ciudades? El futuro es imparable. Lo mismo se aplica al empleo de máquinas para la fabricación o al uso de la telefonía móvil. No hay opción

---

por azar. Pensemos que muchos de los juegos de azar hoy se desarrollan en Internet, y no con un croupier humano, sino con un bot: una máquina, a la que deberíamos aplicarle la ética de la que estamos hablando. Las apuestas por Internet, a diferencia de muchos otros tipos de actividad de juego, son una actividad solitaria, lo que las hace aún más peligrosas: la gente puede jugar sin interrupciones y sin ser detectados por períodos ilimitados de tiempo. Por otra parte, poseen la capacidad para adoptar múltiples identidades falsas en el ciberespacio, lo implica que el bloqueo de cuentas de usuario será ineficaz. Es poco probable pues, que el autocontrol sirva para algo. Y ya que el usuario carece de control sobre sí mismo, ha de ser el sistema, la máquina, en definitiva, quien lo haga (Dudley, 85).

[10] Por ejemplo, pensemos que somos los gestores del tranvía en una ciudad. Una máquina se descontrola, va a descarrilar y el número de muertos puede ser el mayor hasta la fecha en los accidentes de ese estilo. Tenemos una alternativa, que es desviar manualmente el vagón, pero sabemos que al hacerlo irremisiblemente mataremos a una persona, que se encuentra atrapado en el cuarto de máquinas al que accedió para hacer una reparación. ¿Lo desviamos? Ésta pregunta la hice a un grupo de alumnos y masivamente dijeron "si". Ahora introducimos una variación: para desviar el tranvía hace falta que empujemos a una mujer que lleva un carrito de la compra sobre la vía. La respuesta cambia a un "no" sin fisuras.

En ambos casos muere un inocente. Cuando pido que me expliquen el porqué del cambio no aparecen explicaciones racionales. Algunos dicen que son situaciones totalmente distintas. Unos pocos logran justificarlo pero tras un periodo largo de reflexión, mayor que el que la inmediatez para salvar a los pasajeros del tranvía requerían.

La respuesta va dentro de nuestro cerebro de sapien, predispuesto a evitar la violencia innecesaria, a no hacer daño de forma directa e intencional, si no suponen una amenaza directa para nosotros. Es un freno interno y, digámoslo, un maravilloso freno. Es algo que nos hace tomar caminos inmediatamente ante dilemas éticos que se nos presentan a diario. Algunas grabadas en nuestros genes, otras aprendidas y que conforman en día a día de nuestras sociedades.

de retorno. Podemos definir límites, pero no detener el cambio. (Latorre Sentís, 2019). La pregunta del millón es: ¿cómo codificamos esto en un algoritmo?

En enero 2017, convocados por la Conferencia Beneficial Artificial Intelligence 2017 organizado por Future of Life Institute, se reunieron investigadores, científicos y líderes de la industria relacionados con el desarrollo de la Inteligencia Artificial en Asilomar, California, Estados Unidos, quienes analizaron, debatieron y redactaron posteriormente los Asilomar IA Principles conocidos en español como los Principios de Asilomar.

Han sido incluidos en la regulación es el estado de California y la apoyan investigadores principales en inteligencia artificial en google facebook Apple y más de 3800 expertos en inteligencia artificial.

Puede verse un resumen en el anexo.

Robots

El desarrollo de la inteligencia artificial genera progreso en su aplicación, pero su adopción puede plantear ciertos problemas de carácter moral y ético muy relevante, y el problema parece agitarse si le damos forma antropoide o no a esas IA: si les damos forma de robots. No hace falta recurrir a la ciencia ficción, sino a los telediarios, para poder ver que los robots serán más rápidos e inteligentes que nosotros, y que de hecho ya lo son en algunos aspectos, así que debemos esperar conflictos relativos a la integración entre humanos y robots. Una aproximación al problema es desarrollar un conjunto de reglas y normativas de seguridad industrial relativas al despliegue robots industriales en entornos de trabajos compartidos con humanos. (Barrio Andrés, 2018)

Hagamos un poco de historia, para contextualizar la robótica, según (Barrio Andrés, 2018). A finales del S. XVIII y principios del XIX, la Revolución Industrial proporcionó las bases para la construcción de autómatas que pudieran ayudar a mejorar la eficiencia de producción en la industria textil. Los primeros autómatas programables aparecen, y con ellos el importante concepto de programa. En las primeras décadas del XX aparecen mecanismos más o menos autónomos que resultan útiles en distintas industrias. Y también el nombre "robot" de la mano de Karel Capek y, sin abandonar a los escritores de ciencia ficción, es entre este momento y la siguiente revolución cuando Isaac Asimov publica sus tres leyes de la robótica[11], a la que luego añade una cuarta. Es el momento de máxima popularidad. Durante las décadas de 1950 y 1960 aparecen las primeras descripciones de robots en revistas populares y luego industriales, robots de producción o industriales que aún hoy funcionan. Son robots telemanipuladores que precisan de un control continuo de un operador humano. El siguiente paso se desarrolla como una subdisciplina de la robótica: la teoría de control (1970), que viene de la mano del avance de la informática, convirtiendo a los robos en cada vez más autónomos y más inteligentes. (Barrio Andrés, 2018). La polémica aparece y empieza a ser un elemento de interés[12].

[11] La primera: un robot no hará daño a un ser humano ni permitirá con su inacción que sufra daño, ya ha sido claramente violada por el uso de robots de guerra… los drones.

[12] Se recomienda buscar y revisar los siguientes encuentros / documentos:

1. Simposio Internacional sobre robótica (San Remo, Italia, 2004)

Barrio propone tres posibles clasificaciones de los robots: (Barrio Andrés, 2018)

1. Considerando su complejidad: control manual, manipulador, automático programable, capaz de adquirir datos de su entorno.
2. En cuanto a sus componentes: electromecánico, nanobot, softbot.
3. En cuanto a su aplicación: ambiental, cirugía, militar, educación, etc

Los robots son muy mediáticos y no suelen dejar indiferentes. Latorre nos recuerda la polémica suscitada en Arabia Saudí por la obtención de la ciudadanía por la robot Sophia. (Latorre Sentís, 2019)

Una pregunta suele suscitarse: ¿Podemos adoptar esquemas clásicos de la ética en la robótica? Pensemos en el imperativo categórico. Resumamos de forma precipitada que Kant nos dice que hay dos formas de dictar acciones, llamadas imperativos. El primer imperativo es muy frecuente: para sacar un bote de la máquina, mete una moneda. Pero si no tengo sed y no quiero sacar un bote, el imperativo pierde sentido. La mayoría de los imperativos dependen de una condición, y son llamados imperativos hipotéticos. Si la condición no se cumple, el imperativo pierde todo el sentido. Pero hay otro tipo de imperativos: el imperativo categórico. Un ejemplo elemental: no mientas si no quieres que te mientan. Vemos que es una expresión autosuficiente, independiente de nuestras creencias y aplicable siempre. Pensemos ahora sobre la posibilidad de programar a las máquinas inteligentes utilizando como guía el imperativo categórico. Un robot gestionado por una inteligencia artificial se retroalimenta de datos, datos de su propio funcionamiento y datos del exterior que puede comparar y analizar. No parece sencillo incluir imperativos categóricos en esa programación, pero al menos si puede salir un buen debate ético sobre sus criterios de actuación.

Dejemos ahora aparcado a Kant y vamos con el utilitarismo, en un rápido viaje al siglo XVIII de la mano de Jeremy Bentham, quien concluye que estamos dominados por dos fuerzas: placer y dolor. El utilitarismo rompe con Kant, pues las acciones no son buenas o malas por sí mismas. Esto dependerá de las consecuencias que conlleve. ¿Podemos intentar programar una toma de decisiones sobre consecuencias futuras? ¿Inspirándonos en hechos pasados que esperamos que se repitan? ¿Inspirándonos en una experiencia colectiva del pasado? (Latorre Sentís, 2019)

IoT

Entendemos por IoT, Internet de las Cosas o Internet of Things, a la interconexión digital de objetos cotidianos con internet. Sin apenas darnos cuenta, van introduciendo cambios en nuestras vidas (López i Seuba, 2019), como nuevos hábitos que pueden ir del empleo de la domótica a como vemos la televisión (vemos series de televisión con Netflix, HBO, muchas veces con sugerencias tomadas de nuestros hábitos), aparecen nuevos productos (ropa inteligente) y obviamente nuevas consecuencias (medio ambiente) y nuevas posibilidades. Por

2. Programa de ética de la ciencia y la tecnología por la ONU y organización de la educación científica y cultural (UNESCO)
3. Proyecto ethicbots (España, financiado por el 6º Programa Marco de la Comisión Europea)
4. Propuesta del Parlamento Europeo sobre robótica y derecho civil (2017)

ejemplo, ya que hablamos del medio ambiente[13], pensemos en sensores térmicos, sensores de CO2, luces que se pueden apagar solas… incluso edificios inteligentes.

Los elementos del internet de las cosas serían: (López i Seuba, 2019)

1. Objetos o cosas conectados a Internet y entre ellos.
2. Datos generados por los objetos.
3. Procesos conjuntos de fases a los que se les mete algo para transformarlo.
4. Personas.

Obviamente esta interconexión es susceptible de presentar diversos problemas. Éstos los resume (López i Seuba, 2019) en la siguiente relación:

1. Seguridad física. Es uno de los factores más importantes para los gobiernos. No se trata de pensar en recuperaciones ante problemas con el clásico apaga y vuelve a encender. De la Administración Pública depende nuestra vida cotidiana: tráfico, hospitales, escuelas...
2. Privacidad.
3. Otras cuestiones.

La ética aplicada a la IoT puede considerarse una ética de ámbito profesional en tanto que se ocupa esencialmente la responsabilidad de determinados grupos de expertos, pero también tendría una parte de ética empresarial en tanto que dichos expertos trabajan en corporaciones de ámbito privado o público que deben desarrollar una determinada cultura ética que permita tomar decisiones orientadas hacia el interés general de la sociedad o bien común. (Colmenarejo Fernández, 2017)

Big Data

En este apartado vamos a más que seguir tratar de resumir el estupendo trabajo de (Colmenarejo Fernández, 2017) al respecto. Este asunto se esbozó en el tema relativo a protección de datos, así que es posible que se encuentre alguna redundancia en el presente.

La gestión masiva de datos tiene una serie de conflictos a veces éticos, a veces legales, que nos deben hacer repensar algún que otro aspecto. Por ejemplo ¿Quién es el sujeto moral? ¿Qué aspectos del ejercicio profesional tienen dificultades para estar regulados legalmente? Los usuarios no han llegado a comprender cómo afecta las violaciones de privacidad tanto a ellos como individuos como en general, como sociedad. Hay una serie de problemas que, unidos, generan un verdadero peligro. Sumemos la falta de transparencia en las políticas de privacidad de las empresas, la habitual falta de información respecto a los análisis predictivos que se realizan, el empleo de datos falsos que resultan de análisis imperfectos y que pueden ser compartidos en centros de datos, con la dificultad obvia resultante de ejercer el derecho a corregir errores o falsedades y, no solo de datos falsos viene el problema, sino de los perfectos

[13] Escenarios concretos al hablar de medio ambiente e IoT, donde todos tienen en común el uso de la tecnología de la sensorización para obtener datos y realizar acciones correctoras (López i Seuba, 2019)

1. Conservación de la biodiversidad.
2. Caza furtiva y tráfico de especies.
3. Extinción de la fauna salvaje.
4. Restauración ecológica.

resultados de análisis predictivos que determinan con exactitud atributos sensibles como la orientación sexual, origen étnico, creencias religiosas , ideología política e incluso las probabilidades de cometer delitos, mediante las técnicas avanzadas de vigilancia Pre-crimen. (Colmenarejo Fernández, 2017)

Así, podemos resumir en dos los problemas éticos fundamentales que afectan a la gestión de Big Data, siempre según (Colmenarejo Fernández, 2017)[14]:

1. Identidad: la diferencia entre identidad online e identidad offline, e incluso la adopción de otras identidades (como los "prosumers", p.e., esos consumidores de una marca que no se conforman con ser clientes, sino que parecen fundir su identidad con la misma, colaborando con ella).
2. Vulnerabilidades visibles e invisibles en la privacidad. Pensemos en el oxímoron "vigilar para liberar". De paso, esto nos ayudará a comprender los retrasos en la publicación del Reglamento General de Protección de Datos tras la ola de atentados yihaidistas en Europa. Pensemos en esas aplicaciones ya conocidas que permiten reconocer caras entre multitudes en pasos fronterizos, basadas en data mining, estadística y machine learning al tiempo.

Para poder llevar a cabo una correcta gestión en la ética del Big Data (Colmenarejo Fernández, 2017) indica una serie de puntos a considerar:

1. Hay que identificar a los stakeholders.
2. Hay que identificar las implicaciones en la toma de decisiones éticas.
3. Hay que crear un marco para la toma de decisiones, una serie de puntos de decisión ética. Para esto propone una serie de términos:
    a. Conocer la intención: las intenciones finales de aquellos que tienen acceso a los datos.
    b. Verificar la seguridad: medios que la organización tiene para cumplir los requisitos de seguridad establecidos por la ley o por su propia exigencia.
    c. Estudiar la probabilidad: la probabilidad de que existe de que del acceso a datos específicos resulte un beneficio o un daño.
    d. Estudiar posibles agregaciones: la organización debe establecer y hacerse responsable de la combinación de posibilidades derivadas de la correlación de los datos disponibles.
    e. Definir responsabilidades: los distintos grados de obligación que surgen en cada punto de la cadena de datos respecto a la consideración de las consecuencias de la acción.
    f. Localización de identidad: las colecciones de datos correlacionados e interrelacionados que permiten que un sujeto sea caracterizado individualmente.
    g. Estudiar los derechos de propiedad: quién tiene los derechos en cada punto de la cadena de datos.

[14] Básicamente jugamos con cinco factores para tratar de dar luz a todo esto. Son las "5V": volumen, velocidad, variedad, veracidad y valor. (Colmenarejo Fernández, 2017)

h. Cuantificar el beneficio: contribución específica positiva de los datos disponibles a la organización y al usuario
i. Cuantificar el daño: tipo de daño, sobre la identidad, la privacidad, la intimidad o la reputación que podría derivarse del acceso a datos específicos.

Nos queda solo tratar de dos aspectos, también estudiados por (Colmenarejo Fernández, 2017): el cuándo y el cómo. El cuándo se refiere a los momentos del proceso donde hay que estar atentos. Esto es lo que se relaciona como la taxonomía de la vulneración de la privacidad. Con respecto al cómo, nos referimos a los principios que un profesional debe considerar. Veamos estas dos relaciones.

Taxonomía de la vulnerabilidad de la privacidad (Colmenarejo Fernández, 2017):

1. Recolección
2. Proceso: incluye recopilación, identificación, seguridad, usos secundarios y exclusión.
3. Difusión: violaciones de confidencialidad, revelación, exposición indebida…
4. Interferencia en la toma de decisiones e intrusión

Principios profesionales en protección de datos (Colmenarejo Fernández, 2017)

1. Prevención del daño.
2. Desigualdad informativa: p.e. cuando se coloca a personas en desventaja para negociar contratos, p.e.
3. Injusticia informativa y discriminación: información personal proporcionada en un determinado contexto, p.e. en atención médica, que puede cambiar de significado en otro contexto, p.e. en transacciones comerciales.
4. Instrucciones de autonomía moral: se puede exponer los individuos a fuerzas externas que influyen en las elecciones del profesional.

Soluciones propuestas por la Comisión europea.

Algunas de las iniciativas más destacadas que buscan la formulación de principios éticos para la IA y los sistemas "autónomos", provienen de la industria y de los profesionales y sus respectivas asociaciones. (Comisión Europea. Grupo Europeo sobre Ética de la Ciencia y las Nuevas Tecnologías, 2018)

Entre estas iniciativas es importante destacar:

- El tratado "Diseño Éticamente Alineado" del IEEE (Instituto de Ingenieros Eléctricos y Electrónicos)

- La Cumbre Global "IA para el bien" de la IUT (Unión Internacional de Telecomunicaciones)

- La conferencia AAAI/ACM "IA, Ética y Sociedad" (2018).

- "Principios de Asilomar para la IA" (Future of Life Institute) (resumen en anexo)

La comisión presenta lo que denomina una serie de principios éticos y prerrequisitos democráticos precisos para el establecimiento de un marco ético en el ámbito de la inteligencia artificial. Un resumen de los mismos puede verse en el anexo.

Conclusiones

Los sistemas de información, los ordenadores, internet… son herramientas. Como un cuchillo de cocina, buenos o malos según en qué manos sean manejados. No hay ética alguna en ellos, sino en los humanos que los manejan, manipulan o perjudican.

Subiendo un peldaño más y hablando de inteligencia artificial, coincidimos con (Barrio Andrés, 2018) al decir lo mismo de ella. Toda robótica que contribuya en medios y fines a la felicidad y a la Justicia los seres humanos es buena y positiva. A esto, añade una coda de mucho interés: toda robótica que escape del control humano, si estuviese dotada de verdadera inteligencia, estaría abocada a reproducir nuestras mismas imperfecciones.

¿Es posible pues enfocar una ética hacia máquinas que piensen solas? (Latorre Sentís, 2019) nos recuerda que nadie creía que el hombre volaría o que llegaría la luna; que los humanos descubriríamos el código genético, manipularíamos especies o que crearíamos máquinas portentosas. La incapacidad de prever el futuro con lucidez es una constante en la historia de la humanidad. Es pues, no solo posible sino necesario. Incluso, si queremos adentrarnos como parece hacer la UE (Parlamento Europeo, 2017) en la ciencia ficción, sobre las propias máquinas (recordemos esa frase de Arthur Clarke en 2010, Odisea 2: "El estar construido sobre carbono o sobre silicio no constituye una diferencia fundamental; ambos deberíamos ser tratados con el debido respeto")

La historia nos ha dado suficientes pruebas de incapacidad de predicción tecnológica (baste recordar lo que dijo Thomas Watson, presidente de IBM en los años 50: "creo que en el mundo hay mercado para unas cinco computadoras", o un cuarto de siglo después Ken Olson, cuando estaba al frente de la DEC, Digital Equipment Corporation, en 1977 "¿qué motivo puede haber para alguien quiera una computadora en su casa?) Eso nos debería bastar para poder abrir bien los ojos y anticipar de forma generosa lo que puede venir.

La mejor manera de acabar este tema es con una idea de (Barrio Andrés, 2018): Prometeo robó para nosotros el fuego de los dioses. Como mortales no lo utilizamos para convertirnos en dioses. Los dioses no se enojaron con nosotros por querer ser semejantes a ellos. No hay grandes relatos, el mito o la fe en la ciencia deben ceder ante la necesidad vital y realista del discernimiento: "con nosotros con las máquinas, o las máquinas o nosotros. Y esto en cada situación concreta".

Bibliografía

Aigrain, P. (2012). *Sharing. Culture and the Economy in the Internet Age.* Holanda.: University Press.

Barger, R. N. (2008). *Computer ethics: a case-based approach.* NY, EE.UU. : Cambridge University Press.

Barrio Andrés, M. (2018). *Derecho de los robots.* Madrid: Wolters Kluwer.

Brandt, R. L. (2009). *Las dos caras de Google.* Barcelona: Viceversa.

Bynum, T. W., & Rogerson, S. (2004). *Computer ethics and professional responsibility.* Cornwall: Blackwell.

Clarke, R. A., & Knake, R. K. (2010). *Cyber War: The Next Threat to National Security and What to Do About It.* Otawa, Canada: HarperCollins.

Colmenarejo Fernández, R. (2017). *Una ética para Big Data.* Barcelona: UOC.

Comisión Europea. Grupo Europeo sobre Ética de la Ciencia y las Nuevas Tecnologías. (2018). *Declaración sobre Inteligencia artificial, robótica y sistemas "autónomos".* Luxemburgo: Oficina de Publicaciones de la Unión Europea.

Cotino, L. (2008). *Consumidores y usuarios ante las nuevas tecnologías.* Valencia: Tirant Lo Blanch.

Crespo Fajardo, J. L. (2012). *Arte y cultura digital.* Málaga: Eumed.

David, A. (1973). *La cibernética y lo humano .* Barcelona : Labor .

De George , R. (2003). *The ethics of information technology and business.* Cornwall: Blackwell.

Dudley, A., Braman, J., & Vincenti, G. (2012). *Investigating Cyber Law and Cyber Ethics: Issues, Impacts and Practices.* EE.UU.: IGI Global.

Edgar, S. L. (2003). *Morality and Machines. Perspectives on Computer Ethics.* Boston, EE.UU.: State University of New York, Genese. Jones and Bartlett Publishers, Inc.

EUR-Lex. (1 de junio de 2019). *El acceso al Derecho de la Unión Europea*. Obtenido de https://eur-lex.europa.eu/homepage.html

Garriga Domínguez, A. (2012). *Fundamentos éticos y jurídicos de las TIC.* Pamplona: Aranzadi.

Girard, B. (2007). *El modelo Google.* Barcelona: Granica.

Hadnagy, C. (2011). *Social Engineering: The Art of Human Hacking.* EE.UU.: Wiley.

Himanen, P. (2004). *La ética del hacker y el espíritu de la era de la información.* Barcelona: Destino.

Himma, K., & Tavani, H. T. (2008). *EINAR, K. y TAVANI, H. The handbook of information and computer Ethics.* Hoboken, NewJersey, EE.UU.: John Wiley & Sons.

Ippolita, C. (2010). *El lado oscuro de Google. Historia y futuro de la industria de los metadatos.* Barcelona: Virus.

Jennings, M. M. (2009). *Business ethics.* EE.UU.: South-Western.

Jennings, M. M. (2009). *Business Ethics .* N.Y., EE.UU.: South-Western.

Joyanes Aguilar, L. (2010). *Ciberseguridad. Retos y amenazas a la seguridad nacional en el ciberespacio.* Madrid: Ministerio de Defensa.

Khosrow-Pour, M. (2003). *KHOSROW-POUR, M. Annals of Cases on Information Technology. Information Resources Management Association.* Londres, Reino Unido: Idea Group Publishing.

Kshetri, N. (2010). *The Global Cybercrime Industry.* N.Y., EE.UU.: Springer.

Latorre Sentís, J. (2019). *Ética para máquinas.* Barcelona: Ariel.

Laudon, J. P., & Laudon, K. C. (2016). *Sistemas de Información Gerencial.* Madrid: Pearson.

Lessig, L. (2001). *El código y otras leyes del ciberespacio.* Madrid: Taurus.

Libicki, M. C. (2009). *Cyberdeterrence and cyberwar.* N.Y., EE.UU.: RAND.

Livingstone, S. (2009). *Children and the internet .* Cambridge : Polity Press .

López i Seuba, M. (2019). *Internet de las cosas. La transformación digital de la sociedad.* Madrid: Ra-Ma.

Mitnick, K. D., & Simon, W. L. (2007). *El arte de la intrusión.* Madrid: RA-MA.

Mitnick, K., & Simon, W. (2011). *Ghost in the wires.* EE.UU.: Little, Brown and Company.

Mitnick, K., & Vamosi, R. (2018). *El arte de la invisibilidad.* Madrid: Anaya.

Parlamento Europeo. (2017). *Normas de Derecho civil sobre robótica.* Estrasburgo: Parlamento Europeo.

Porter, E. (2011). *Todo tiene un precio: Descubre que el valor de las cosas afecta al modo en que nos enamoramos, trabaja.* Madrid: Aguilar.

Reischl, G. (2008). *El engaño Google.* Madrid: Medialive.

Smoller, J. (2014). *La otra cara de lo normal.* Barcelona: RBA.

Stallman, R. M. (2004). *Software libre para una sociedad libre.* Madrid: Traficantes de Sueños .

Stoll, C. (1990). *El huevo del cuco.* Barcelona: Planeta.

Suarez Sánchez-Ocaña, A. (2012). *Desnudando a Google.* Madrid: Deusto.

Vázquez, J. M., & Barroso, P. (1996). *Deontología de la informática (esquemas).* Madrid: Instituto de Sociología Aplicada.

Contenido

Tema 9. TIC, Sociedad, Profesión y Ética: una confluencia necesaria. 1
Introducción 1
Un poco de historia. 3
Definiciones 3
Ética informática y profesional informático 5
La ética en los proyectos informáticos. 7
Deberes del profesional informático 9
Dimensiones morales 12
Derechos y obligaciones de información: 13
Derechos y obligaciones de propiedad: 14
Rendición de cuentas y control: 17
Calidad del sistema: 18
Calidad de vida: 19
Códigos éticos en relación con la informática 20
Una figura polémica. Hackers, hacking. 21
Trastornos y enfermedades derivadas de las TIC 27
De la robótica a la Inteligencia Artificial ¿un cambio de ética? 29
Profesionales e IA. 30
Toma de decisiones por la IA 31
Sistemas autónomos 32
Robots 34
IoT 35
Big Data 36
Soluciones propuestas por la Comisión europea. 38
Conclusiones 39
Bibliografía 39