CUESTIONES ETICAS PROBLEMÁTICAS EN LA ERA DE LA INFORMACION, INTERNET Y LA WORLD WIDE WEB

Por

Luisa Montuschi[*]

RESUMEN

Los avances en la tecnología de la computación presentan tanto oportunidades como peligros a las personas, las organizaciones y la sociedad en su totalidad. La tecnología y sus aplicaciones a la vida laboral y privada de los individuos constituyen desafíos para muchos valores sociales arraigados. Las nuevas cuestiones éticas que han surgido demandan respuestas. Las principales preocupaciones se refieren a los temas de privacidad, vigilancia en el lugar de trabajo, propiedad, seguridad, acceso y poder. El carácter crecientemente global de Internet y de la World Wide Web requiere de normas morales globales y de responsabilidad profesional. El principal desafío sería encontrar la manera que los valores sociales y éticos pudiesen ser incorporados en la nueva sociedad global de la tecnología digital.

ETHICAL ISSUES IN THE AGE OF INFORMATION, INTERNET AND THE WORLD WIDE WEB

ABSTRACT

Advances in computer technology present many opportunities as well as dangers to individuals, organizations and the society as a whole. Many social values are challenged by the technology and its application to the work and private life of many individuals. New ethical issues have arisen that should be dealt with. The primary concerns are the problems of privacy, surveillance in the workplace, property, computer security, access and power. The increasing global character of Internet and the World Wide Web requires global moral norms and professional responsibility. The main challenge is to find a way in which social and ethical values could be incorporated in the new global society of digital technology.

[*] Las opiniones expresadas en este artículo son del autor y no necesariamente reflejan las de la Universidad del CEMA.

CUESTIONES ETICAS PROBLEMÁTICAS EN LA ERA DE LA INFORMACION, INTERNET Y LA WORLD WIDE WEB

Por

Luisa Montuschi

"It's impossible to move, to live, to operate at any level without leaving traces, bits, seemingly meaningless fragments of personal information."

William Gibson

"The advance of technology is based on making it fit in so that you don't really even notice it, so it's part of everyday life."

Bill Gates

Las tecnologías de la información y de la comunicación (TIC) están invadiendo todos los aspectos de la existencia humana y están planteando serios desafíos a valores sociales que se consideraban firmemente establecidos. Es cierto que las tecnologías de la computación, Internet y la World Wide Web han creado posibilidades a nivel global que no estaban antes disponibles ni para los individuos ni para las organizaciones. Pero también es cierto que han surgido nuevas cuestiones éticas porque los cambios están afectando las relaciones humanas, las instituciones sociales y principios morales básicos que se espera tengan vigencia en las distintas sociedades y culturas.

La nueva sociedad basada en las tecnologías de la información y de la computación debería constituirse en un instrumento para la integración social, para formar una sociedad coherente e inclusiva. Debería tender a reducir las desigualdades existentes y asegurar el acceso general a la información y a los servicios. Es indudable que esta sociedad presenta un enorme potencial y habrá de ofrecer muchas oportunidades que es necesario identificar y para las cuales es indispensable formarse. Su desarrollo no puede constituir sólo una expansión de la infraestructura de la información y de la comunicación. Deberá tratarse de una sociedad informada y participativa que transcienda de la noción tecnocéntrica para adquirir una dimensión humana en la cual el conocimiento compartido constituya la base de la cohesión social.

El mundo está sujeto a un cambio casi permanente originado en las nuevas tecnologías. Muchos de esos cambios pueden ser considerados como

positivos. Y, sin duda, para algunos lo han sido y lo serán en el futuro. Otros han sido perdedores a lo largo del proceso. Esto ha llevado a plantear una suerte de dicotomías vinculadas con estos procesos. Así se mencionan los que tienen y los que no, los ricos en información y los pobres en información, los viejos y los jóvenes, los desarrollados y los en desarrollo, los *online* y los *offline*, los usuarios y los desarrolladores, los alfabetos en computación y los iliteratos en computación, los locales y los globales. El mundo de las TIC parece haberse segmentado en muchas partes.

Sin embargo, también es cierto que los nuevos problemas éticos que ya se han presentado y que siguen surgiendo a una velocidad que en muchos casos parece superar la propuesta de soluciones, requiere un análisis particularizado que podría centrarse en las cuestiones referidas a privacidad, control de trabajadores, propiedad, seguridad, acceso y poder, globalización, responsabilidad moral y profesional.

i. Privacidad

Este ha sido, probablemente, el primer tópico que se planteó en relación con las nuevas tecnologías y aquel que ha recibido mayor atención por parte de la opinión pública. Al comienzo la preocupación se centraba en la posibilidad de abuso por parte de las autoridades públicas respecto del ingente acervo de información, referida a los ciudadanos, que las mismas habían recolectado a lo largo del tiempo. Las nuevas tecnologías permitían acceder a cantidades de datos y operar con los mismos con alcances y velocidades antes inimaginables. La preocupación se presentó en los Estados Unidos cuando los intentos de reunir toda la información individual (datos censales, impuestos, servicio militar, ayuda social, etc.) bajo un único número de identificación despertó una reacción pública adversa atemorizada por una posible intervención tipo “gran hermano”. En definitiva, tales intentos fueron abortados en su mismo origen. De hecho, ello obligó a aprobar un cuerpo de legislación tendiente a proteger la privacidad de información eventualmente amenazada por la creciente utilización de las computadoras.

Pero, la muy rápida evolución de las tecnologías, la baja en los costos de dichas tecnologías, la aparición de software amigable para el usuario, la difusión de Internet, la casi general utilización del correo electrónico,

el desarrollo de nuevos instrumentos computerizados para el monitoreo en los lugares de trabajo, los avances en los procesos de control por parte de agencias de inteligencia, han planteado y siguen planteando serias preocupaciones en la población que parece avizorar una creciente invasión de su intimidad a través de muy distintos canales difíciles de evitar.

En principio no aparece demasiado claro qué se entiende por privacidad, en particular en vista de todos los desarrollos mencionados más arriba. Un antecedente podría ser lo enunciado en la Declaración Universal de Derechos Humanos de las Naciones Unidas en 1948 que en su artículo 12 estipula que "nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia... Toda persona tiene derecho a la protección de la ley contra tales injerencias...". Pero esto resulta hoy claramente insuficiente.

De George hace notar que la noción de privacidad es relativa, ya que varía de manera considerable de una sociedad a la otra[1]. En los primeros análisis referidos a ese tema aparece como clásica una definición dada por Warren y Brandeis que identifican la privacidad como "el derecho a ser dejado solo" y sostienen que las leyes deberían proteger "la privacidad de la vida privada"[2]. Boatright, y también otros críticos, encuentran la definición a la vez demasiado amplia en ciertos aspectos y estrecha en otros. Y se supone que ello se debe a que se confunde el concepto de privacidad con el de libertad. Se reconoce como mejor una definición en la cual la privacidad se expresaría en términos de control respecto de la información acerca de uno mismo. Al parecer, una mejor definición sería la dada por W.A. Parent quien define la privacidad como "la condición de que el conocimiento personal no documentado acerca de uno mismo no pueda ser poseído por otros". Y por conocimiento personal se entiende a aquellos hechos que la mayoría de las personas, en cualquier sociedad y tiempo, no desean que sean ampliamente conocidos[3].

---

[1] Cf. De George, R.T., **Business Ethics,** Prentice Hall, 1999.

[2] Citado en Boatright, J.R., **Ethics and the Conduct of Business,** Prentice Hall, 2003.

[3] Cf. Parent, W.A., "Privacy, Morality and the Law", **Philosophy and Public Affairs**, Vol. 12, 1983.

Bynum señala que desde la década del sesenta se ha avanzado en el desarrollo de una teoría de la privacidad definida como el ”control sobre la información personal”[4]. Pero otros autores han señalado que esa concepción es claramente insuficiente y más que de control habría que referirse a “acceso restringido”[5].

Boatright considera que en sus análisis el concepto de privacidad se limita a las cuestiones que implican la información en el sentido planteado por Parent. De George, por su parte, manifiesta que el concepto se refiere a muchas acciones y casos pero que lo pertinente en materia de las nuevas tecnologías tiene que ver con la privacidad de la información y la privacidad electrónica. La primera es coincidente, en gran medida, con la concepción de Parent y la problemática se agudiza con el hecho de que en el presente mucha información personal está guardada en bases de datos en computadoras. Muchas personas pueden tener acceso a dichas bases, algunas en forma autorizada y otras, de modo crecientemente sencillo, en forma no autorizada.

En cuanto a la privacidad electrónica la misma está vinculada con el uso del e-mail y de Internet por parte de los trabajadores en su lugar de trabajo. Estos esperan que el correo electrónico tenga el mismo nivel de protección que tiene el correo común. Y ello no es así toda vez que se utilizan computadoras propiedad de la empresa. Al respecto no parece existir una regla ética obligatoria. Incluso en los Estados Unidos la justicia ha determinado que al ser las computadoras propiedad de las empresas, éstas podrán determinar libremente cual será su política respecto de la privacidad del e-mail: respetar la privacidad de los e-mails, salvo en caso de ser requerida información por agencias gubernamentales, o disponer el acceso ilimitado a los mismos por parte del management o de los supervisores.

Sin embargo, se considera que sería correcto que las empresas informaran a sus empleados respecto de tal política para que los mismos no operen bajo la creencia errada de que sus e-mail gozan de un derecho a la

[4] Cf. Bynum, Terrell Ward, "Computer Ethics: Basic Concepts and Historical Overview", **The Stanford Encyclopedia of Philosophy** (Winter 2001 Edition), Edward N. Zalta (ed.), URL = <http://plato.stanford.edu/archives/win2001/entries/ethics-computer/>.

[5] Cf. Tavani, H.T. y Moor, J.H., “Privacy Protection, Control of Information, and Privacy-Enhancing Technologies”, **Computers and Society**, Vol.. 31,Nº 1, 2001.

privacidad que, en realidad, no tienen. Por otra parte, las empresas deberían tener claro que los trabajadores habrán de considerar que una política de libre acceso a sus mails implicaría una clara muestra de desconfianza por parte de la organización.

Respecto del acceso a Internet en el lugar de trabajo el planteo es similar al efectuado respecto del e-mail en el sentido de que las empresas pueden decidir acceder al uso que del mismo se ha hecho. Pero, además, existen dos cuestiones adicionales que también resultan problemáticas: el abuso en la utilización del tiempo y el acceso a sitios no vinculados con el empleo y aun a sitios inconvenientes o ilegales (pornografía, pedofilia, terrorismo).

Debe tenerse presente que los problemas de privacidad no se presentan en forma exclusiva en los lugares de trabajo. También en el hogar y en otras circunstancias pueden producirse invasiones a la privacidad que, por cierto, no están reguladas o controladas por la ley. La evolución de las tecnologías de la información ha incrementado notoriamente la capacidad de vigilancia, comunicación, intervención, acumulación, almacenamiento y recuperación de información, sin que el interesado sea necesariamente consciente de tales situaciones. Y lo que vuelve la cosa más sería es el hecho de que la información tiene un valor creciente en nuestra sociedad y es una fuente de poder. Parafraseando a Sir Francis Bacon podríamos decir que "la información es poder"[6]. En esta sociedad de la información la misma constituye un activo crecientemente valioso para los hacedores de políticas. Y es bien cierto que no todo el mundo es plenamente consciente de cuanta información respecto de nosotros mismos debe figurar actualmente en muchas bases de datos públicas y privadas. Y tampoco podemos tener seguridad alguna de que dicha información sea realmente correcta ni se puede determinar quien o quienes tendrán acceso a la misma y con qué propósitos.

Por otra parte, los cambios se producen tan rápido que resulta muy difícil seguirles los pasos y establecer salvaguardias que resulten efectivas. Aquí se plantean claros dilemas. Por una parte, la posibilidad de tener fácil

[6] La cita de Sir Francis Bacon es *"Ipsa scientia potestas est".*

acceso a la información personal puede facilitar las cosas en materia de trámites y aún de búsqueda de personas. Pero ello es al precio de una clara amenaza a la privacidad e intimidad que lamentablemente no puede ser controlada. Es maravilloso tener la posibilidad de conectarse con personas en cualquier lugar del mundo en forma casi instantánea: parientes, amigos, colegas. Tener acceso a diarios, revistas, artículos generales o profesionales especializados. Comprar libros y otros bienes online no disponibles en el propio país. Es como tener el mundo al alcance de la mano. Pero todo ello tiene un costo, una contrapartida de la cual hay que tener conciencia.

ii. Control y vigilancia en el lugar de trabajo

Estrechamente vinculada con el problema de la privacidad, pero con elementos claramente diferenciados, es toda la problemática referida al control y vigilancia en el lugar de trabajo. Esta cuestión no es nueva pero ha adquirido dimensiones insospechadas con el desarrollo de las nuevas tecnologías de la información. Y, por otra parte, la vigilancia y control pueden ser fácilmente extendidos más allá del ámbito laboral y llegar incluso al hogar o a otras actividades que se llevan a cabo más allá de las correspondientes a los respectivos empleos.

En el pasado los controles también se llevaban a cabo. Pero los mismos estaban a cargo de personas, generalmente supervisores o capataces, que estaban bien a la vista de los controlados. No había ocultamiento ni ambigüedad en esa actividad. De hecho, algunos autores quieren ver en la presente actividad de vigilancia una suerte de continuación del “taylorismo” en el cual los supervisores controlaban que se cumpliera con los tiempos y estándares que los procesos de producción masiva requerían.

Sin embargo, existe una clara diferenciación de fondo ante ambos procesos de control ya que en el presente los procesos de control tienen razones y motivaciones que difieren de las correspondientes a los anteriores procesos. Tal vez la única coincidencia podría encontrarse en el hecho de que en ambos casos una de las razones aducidas es la referida al logro de una mayor productividad y eficiencia en los procesos. Pero, en el presente tal deseo se contrapone con la demanda de privacidad del empleado que, en muchos

casos, puede verse seriamente afectada por las acciones del empleador que podrían llegar a exceder el ámbito meramente laboral.

Las argumentos y razones aducidas por los empleadores para realizar los monitoreos laborales son sin duda razonables. Son los excesos los que no tienen justificación. Tal como se señalara más arriba, la principal razón es la referida a la productividad. Se sospecha siempre que el trabajador dedica buena parte de su tiempo a actividades en su propio interés y, aun se aleja de su lugar de trabajo. En segundo lugar, aparece el deseo y derecho del empleador de protegerse a sí mismo y a su propiedad de los riesgos que la actividad extralaboral del empleado le puede generar y defenderse también de posibles demandas. En tercer lugar, se ubica el control que se quiere ejercer sobre la posibilidad de espionaje realizado, en forma consciente o inconsciente, por el empleado. Luego se suelen mencionar razones vinculadas con el control de desempeño de los trabajadores, con la posibilidad de acoso entre supervisores y empleados o entre los empleados mismos, con la búsqueda de datos extraviados, con el uso de software ilegal o, meramente, para prevenir el uso personal de las computadoras de la empresa por parte de los trabajadores.

Estas situaciones de vigilancia no crean un ambiente favorable de confianza entre el management y los trabajadores de una empresa. Por el contrario, se genera un clima de sospecha y aun de resentimiento que no resulta, por cierto, favorable para la búsqueda de la productividad y la eficiencia que son, en definitiva, las principales razones aducidas para el monitoreo.

En casos extremos de vigilancia se ha llegado a límites que afectan ciertamente a la privacidad de los empleados. Ello se ha dado cuando, por ejemplo, se ha pretendido ejercer vigilancia encubierta en vestuarios, baños o cuartos de recreación de los trabajadores en los cuales ellos esperaban disfrutar de privacidad. Por otra parte, debe tenerse en cuenta que en la actualidad los empleados permanecen en su trabajo por horarios prolongados que les hacen imposible tener la posibilidad, antes o después del empleo, de realizar una multitud de trámites bancarios, comerciales, médicos y otros. En tal caso, resulta comprensible la necesidad de utilizar en horario de trabajo recursos informáticos de la empresa sin que por ello se los deba espiar y recriminar. Finalmente existen algunas modalidades de monitoreo que no

parecen aceptables, o que por lo menos han generado una multitud de quejas. Entre ellas puede mencionarse una iniciativa de empresas mayoristas británicas proveedoras de supermercados y tiendas que obligan a sus trabajadores a usar pequeñas computadoras que se usan como brazales y en el dedo[7]. Estas computadoras los dirigen vía satélite a los estantes del depósito donde están los productos que deben despachar a los minoristas. Estos aparatos incrementan la productividad de los trabajadores y bajan los costos al eliminar los tiempos muertos ya que los dirigen en el recorrido que deben hacer y fijan el tiempo que deben emplear. El debate se plantea entre los sindicatos que sostienen que el uso de estas computadoras convierte a los trabajadores en autómatas que no pueden tener iniciativas y que sólo siguen las instrucciones del aparato, que, por otra parte, puede determinar qué está haciendo en cada momento de su jornada laboral, y las empresas que argumentan acerca del supuesto efecto positivo que esta tecnología tiene sobre la moral de los equipos de trabajadores al facilitarles la tarea. También sostienen que la misma no se utiliza con un propósito de control o vigilancia. ¿Pero quién fija el límite?

En tales casos está presente un dilema de difícil solución. ¿Cómo compatibilizar el derecho a la privacidad del trabajador con el derecho que el empleador tiene de ejercer control sobre el lugar de trabajo y el uso que se hace del mismo. Aquí parecería evidente la necesidad de normas que regulen las formas en que pueden ser utilizadas las nuevas tecnologías. Y, sobre todo deberán tenerse presente dos principios éticos fundamentales. Por un lado, reconocer que por el hecho de que algo “pueda” hacerse no implica que “deba” hacerse. El segundo se refiere a la versión del imperativo categórico de Kant que sostiene que “las personas deben considerarse siempre como un fin y nunca como un medio”.

Pero estas formas de control que plantean tales dilemas han surgido porque los avances tecnológicos las han hecho posibles. Y estos avances

[7] Las principales cadenas de supermercados británicos, Tesco y Sainsbury’s, las grandes tiendas Marks & Spencer, la cadena de farmacias Boots y Homebase, otra cadena que vende artículos para la jardinería y las actividades en el hogar, han adoptado estos aparatos que ya estarían usando entre cinco mil y diez mil trabajadores.

parecen no cesar y vuelven cada vez más barata la instalación de aparatos que posibilitan la vigilancia.

Muchos de los aparatos utilizados se vinculan con el uso de computadoras y pueden monitorear su utilización por los usuarios, observar que archivos se han bajado, filtrar el acceso a ciertos sitios y prohibirlo a otros. También determinar cuanto tiempo se ha permanecido en los mismos[8]. También se controlan los llamados telefónicos[9]. Además se siguen utilizando los más tradicionales sistemas de vigilancia por video y audio. Pero, hay que considerar el hecho de que los aparatos que utilizan microprocesadores pueden ser cada vez más pequeños y más poderosos. En consecuencia, podrían ser ubicados en lugares no detectables y ser activados a distancia sin que el trabajador sepa que se lo está vigilando.

Además de estos productos, que no aparecerían como demasiado revolucionarios, las empresas dedicadas a la seguridad están desarrollando, para su venta en el mercado, productos para la identificación biométrica de usuarios basados en la identificación de ciertas características individuales como las impresiones digitales, caligrafía, voz, ritmos de mecanografiado, geometría de la mano y patrones distintivos de las retinas de las personas. Debe notarse que en caso de que se utilicen tecnologías de tipo biológico para controlar al trabajador, las mismas pueden afectar su privacidad fuera del trabajo.

Es indudable que estas actividades de vigilancia generan un conflicto, difícil de resolver, entre los intereses del empleador y los del trabajador. El conflicto se plantea entre el derecho del empleador a conocer lo que sucede en el lugar de trabajo y a proteger su propiedad y el derecho del trabajador a la protección de su privacidad. Para evitar o minimizar esta contraposición de intereses se han sugerido una serie de pautas que sería necesario que los

[8] Algunos productos que realizan estas funciones son, entre otros, WebSense, New Access Manager, WebTrack e Internet Watchdog.

[9] En la encuesta anual de 2001 de la American Management Association se registraba un importante aumento en la actividad de control y vigilancia aunque la misma se centraba sobre todo en las computadoras e Internet y, sobre todo, el e-mail. En mucha menor medida se controlaban las comunicaciones telefónicas, tarea más difícil y consumidora de tiempo.

empleadores cumplieran, incluso para que los empleados no consideren a la tecnología como un enemigo a combatir[10]. Un primer punto a considerar es el referido a la necesidad de informar a los trabajadores con antelación respecto del hecho de que van a ser controlados. Luego sería necesario observar los puntos siguientes:

1. Recolectar únicamente información pertinente al empleo y limitar el control al lugar de trabajo evitando lugares muy privados como los baños o los vestuarios.
2. No realizar monitoreos secretos.
3. Facilitar a los trabajadores el pleno acceso a la información recolectada referida a ellos mismos.
4. Requerir a los trabajadores que verifiquen la información obtenida antes de que la misma sea utilizada para evaluaciones del personal y evitar discriminación alguna basada en actividades extralaborales.
5. Aplicar un "estatuto de limitaciones" a la información recolectada, en el sentido de que se establezcan fechas ciertas de caducidad de la misma.
6. Requerir que el control obedezca al logro de intereses comerciales ciertos para la empresa.

Sin embargo, existen casos en los cuales parece aceptarse el derecho del empleador a controlar al trabajador, aun en caso de no contar con el consentimiento del mismo[11]. Esto sería posible en el caso en que el control se realice ya sea para registrar transacciones comerciales, para asegurar el cumplimiento de normas regulatorias, mantener efectivas las operaciones del sistema y los estándares de entrenamiento y servicios. Y, como es natural, para prevenir o detectar actividades criminales o el uso no autorizado de las tecnologías del lugar de trabajo.

[10] Cf. Marx, G.T. y Sherizen, S., "Monitoring On The Job: How to Protect Privacy as Well as Property", **Technology Review**, Noviembre-Diciembre 1986 y Hartman, Laura P., "Technology and ethics: privacy in the workplace", **Business and Society Review**, vol. 106 (no. 1), 2001.

[11] Se trataría de vigilancia "encubierta" que en algún país (Australia) es considerada una ofensa, a menos que la misma haya sido autorizada por una autoridad competente.

Al principio todas las actividades de vigilancia y control estaban rodeadas por un aura de temor que, según mencionamos, podían englobarse en el llamado "síndrome del gran hermano" cuando a las mismas se las vinculaban con alguna autoridad pública. Pero los desarrollos tecnológicos relacionados con la vigilancia han tenido características de miniaturización y baja de precios y se han generalizado de tal manera que las posibilidades de hacer uso de los mismos puede estar casi al alcance de cualquiera. Es así que, como señala el Economist, en la nueva sociedad que está surgiendo ya no será sólo el "gran hermano" quien esté observando sino también una multitud de "pequeños hermanos"[12].

iii. Propiedad

La cuestión de los derechos de propiedad, en el contexto de las nuevas tecnologías de la información y comunicación, es probablemente una de las más controvertidas. La problemática se plantea tanto en relación con el software como con los datos y también con el tiempo de computación.

En el pasado la propiedad estaba constituida por cosas tangibles, objetos corpóreos que se podían tocar y, eventualmente, trasladar de un lugar a otro. Hoy el principal activo es la información y, en una segunda etapa, el conocimiento. ¿Pueden ser poseídos la información y el conocimiento? ¿Puede hablarse de un derecho a conocer? ¿Un programa, un algoritmo, una base de datos pueden ser objeto de propiedad privada? ¿No existe una contradicción con el cada vez más amplio acceso en la Web y el deseo de restringir la posesión de mucha información y software que por ella circula?

Estas son algunas de las muchas preguntas a las cuales parece necesario encontrarles una respuesta. Y esto ha dado lugar a un sinfín de controversias. Por un lado, hay que establecer claramente una diferenciación entre los conceptos de datos, información y conocimiento que, en muchos análisis, parecen ser utilizados de manera indistinta[13]. Luego habría que

[12] Cf. The Economist, "Move over, Big Brother", 12 abril de 2004.

[13] Cf. Montuschi, L., "Datos, información y conocimiento. De la sociedad de la información a la sociedad del conocimiento", **Serie Documentos de Trabajo de la Universidad del CEMA,** Nº , 192, julio 2001 y "El conocimiento tácito y el conocimiento codificado en la economía basada en el conocimiento", **Anales de la Academia Nacional de Ciencias Económicas**,Vol. XLVII, Buenos Aires, 2002.

determinar con cierto grado de precisión a cual de esos conceptos nos estamos refiriendo cuando hablamos de eventuales derechos de propiedad.

Se ha dicho que la generación de datos no estructurados no conduce de modo automático a la creación de información y que la información no puede ser considerada automáticamente como conocimiento. Para que ello sucediera, sería necesario que se la clasifique y procese. Del análisis y reflexión respecto del producto obtenido surgirá el conocimiento. En el proceso de generación del mismo, los datos y la información constituyen materias primas de naturaleza intangible.

Algunos autores han procurado diferenciar claramente estos conceptos. Así se ha dicho que datos son la materia prima en bruto, que pueden existir en cualquier forma (utilizable o no) y que no tienen un significado por sí mismos[14]. Otros adoptan una posición epistemológica particular al definir datos como "todos los hechos que pueden ser objeto de observación directa". A continuación definen hecho como "todo aquello que ha sucedido realmente". En este sentido se estaría adoptando la posición del empirismo que supone que existe una realidad externa a la mente humana que puede ser objeto de sensaciones y de mediciones. También se ha dicho que los datos son hechos no estructurados y no informados que existen en forma independiente del usuario[15].

En cuanto a la información parece necesario establecer sin ambigüedades su diferencia con el conocimiento dado que, con frecuencia, a ambos términos se les asigna el mismo significado. Desde la imprescindible definición dada por Fritz Machlup que veía la información como a "un flujo de mensajes o significados que pueden añadir, reestructurar o cambiar el

[14] Cf. Bellinger, G., Castro, D. y Mills, A., "Data, Information, Knowledge and Wisdom", <www.outsights.com/systems/dikw/dikw.htm>,1997.

[15] Los datos serían "unstructured, uninformed facts so copiously given out by the computer. Data can be generated indefinitely; they can be stored, retrieved, updated and again filed. They are a marketable commodity ... each year the cost for data acquisition grows on the erroneous assumption that data are information" Cf. Schoderbek, C.G., Schoderbek, P.P. y Kefalas, A.G., **Management Systems. Conceptual Considerations**, Business Publications, Dallas, 1990.

conocimiento"[16], se ha diferenciado la información de los datos y del conocimiento de varios modos posibles.

Así se ha dicho que los datos se transforman en información cuando son interpretados por quien los recibe y que la información es descriptiva mientras el conocimiento es predictivo[17]. También se ha dicho que la información son los datos que tienen "valor" y que el valor informativo depende del contexto. Por lo tanto, mientras no se ubican los datos en el contexto apropiado no se convierten en información y si el contexto desaparece también lo hace la información. Otro criterio señala que la información son datos a los cuales se les ha asignado significado por medio de una conexión relacional.

También se ha señalado que la distinción entre conocimiento e información corresponde a la diferencia entre un stock y un flujo. Si bien esta afirmación puede ser considerada como una metáfora útil para el análisis, la misma no debería ser tomada en forma literal[18]. En tal sentido, K. Boulding señalaba que el conocimiento no puede ser visto como la acumulación de una pila de información, sino como una estructura muy compleja con sus partes conectadas de varias maneras con ataduras diversas. Los mensajes o señales que constituyen la información bombardean continuamente la estructura. Algunos pasan a través de intersticios sin afectarla, otros se adhieren y pasan a formar parte de la misma. Ocasionalmente aparece algún mensaje que resulta inconsistente con la estructura pero que no puede ser desechado por falso. En ese caso, la estructura debe sufrir un proceso completo de reorganización para resultar consistente con la nueva información[19]. Sin embargo, como hace notar

---

[16] Cf. Machlup, F., "Semantic Quirks in Studies of Information", en Machlup F. Y Mansfield U., (Eds.), **The Study of Information**, **Interdisciplinary Messages**, New York, John Wiley,1983.

[17] Cf. Kock, N.F., Jr., McQueen, R.J. y Corner, J.L., "The Nature of Data, Information and Knowledge Exchanges in Business Processes: Implications for Process Improvement and Organizational Learning", **The Learning Organization**, Vol.4, Nº 2, 1997. Existe una errada interpretación epistemológica del conocimiento al separar los aspectos descriptivos de los predictivos.

[18] Cf. Langlois, R. y Garrouste, P., "Cognition, Redundancy, and Learning in Organizations", trabajo presentado a la **Conference on Evolutionary Economics and Technological Change**, 6-8 octubre 1994, Estrasburgo, Francia.

[19] Cf. Boulding, K., "Notes on the Information Concept", **Explorations,** (Toronto), 6, 1955.

Machlup, todo tipo de experiencia, impresiones accidentales, observaciones e incluso "introspecciones internas" no inducidas por estímulos exteriores, pueden dar comienzo a procesos cognitivos que conducen a cambios en el conocimiento de una persona. En tal caso el conocimiento puede haberse adquirido sin haber recibido información adicional[20].

De acuerdo con lo anterior puede formularse un ordenamiento jerárquico de los tres conceptos analizados:

datos ⇨ información ⇨ conocimiento

donde cada nivel es construido sobre la base del anterior. Pero debe tenerse presente que, en general, el punto de partida para la generación de nuevo conocimiento es el stock de conocimiento ya aceptado y que no todos los datos e información disponibles contribuyen a la construcción de nuevo conocimiento. En consecuencia podríamos formular el proceso de la siguiente manera:

conocimiento ⇨ datos ⇨ información ⇨ conocimiento

⇩ ⇩ ↘ nuevo conocimiento

donde las flechas hacia abajo indican los mensajes (datos o información) que se escurren por los intersticios de la estructura (conocimiento) sin afectarla ni agregar nada nuevo. Las flechas horizontales son aquellos que se adhieren a la estructura (conocimiento inicial) y que aumentan el stock de conocimiento. La flecha inclinada ↘ representa aquellos mensajes que aportan algo nuevo que resulta inconsistente con la estructura inicial y que obligan a un proceso completo de reorganización de la misma.

Aquí habría que plantearse qué parte de ese proceso pueda ser considerado propiedad exclusiva de quien o quienes le dan origen. Y cabe formularse algunas preguntas. Si se parte de un conocimiento que está libremente disponible los datos que se le agregan al mismo para generar nueva información ¿serán propiedad de alguien o deberían ser libremente accesibles? ¿Y si se partiera de un conocimiento que no estuviera libremente disponible? A pesar de que con frecuencia, tanto en los diccionarios como en la bibliografía

[20] Cf. Machlup, F., **Op.Cit.,** 1983.

más especializada, se confunden los conceptos de datos, información y conocimiento existe una notoria diferencia entre los mismos. El mero acceso a cantidades cada ver mayores de datos y aun de información no asegura por sí mismo el crecimiento del conocimiento. Por un lado, buena parte de esos datos pueden ser (sin duda son) de aquellos que se escurren entre los intersticios y, además, resulta posible que la cantidad de tiempo que insume el navegar en medio de tan impresionante caudal, para poder desechar lo que no sirve, reduzca en forma considerable el tiempo disponible para pensar y sí sirve para agregar al conocimiento existente[21].

De acuerdo con lo anterior parecería claro que no debería considerarse la propiedad exclusiva de los meros datos. Una vez que esos datos se hayan convertido en información, ya sea mediante un proceso de clasificación, procesamiento o interpretación, ya no puede ignorarse el problema de la propiedad.

En varios países se han seguido distintas políticas con el propósito de defender la propiedad tanto del hardware como del software. Así, por ejemplo, en Japón la protección se ha dado en ambos casos mediante el uso de patentes. En cambio, en los Estados Unidos al comienzo se había decidido proteger con derechos de autor el software y con patentes el hardware. Pero más recientemente algún tipo de software fue patentado[22]. Sin embargo, dado que tanto los derechos de autor como las patentes fueron desarrollados para productos muy diferentes de los relacionados con las computadoras una infinidad de problemas se han planteado que aún no han tenido una respuesta completamente satisfactoria. Así, solamente a título de ejemplo, podemos señalar algunas de las cuestiones problemáticas y controvertidas. Los datos y programas cargados en una computadora pueden ser considerados propiedad del dueño de la computadora. Pero, qué alcances tiene realmente dicha propiedad. En la medida que el programa ha sido comprado ¿puede ser

[21] El tener acceso a muchos datos e información no vuelve más sabia a la gente y en la actual sociedad, rica en medios masivos de comunicación, desde el punto de vista de los receptores la información se parece más al caos que a los hechos. El receptor debe reconstruir el significado de lo que recibió (conocimiento explícito más conocimiento tácito del autor) mediante un proceso basado en su propio conocimiento tácito.

[22] Cf. De George, R., **Op.Cit.**

reproducido libremente? Al parecer aquí la ley debe intervenir para fijar normas que impidan que se piratee la propiedad ajena. Pero las situaciones son muy variadas y no admiten una solución general. En muchos casos hay programadores que intercambian sus programas o permiten que sean reproducidos libremente. Otros reclaman su exclusiva propiedad aunque no hayan obtenido los derechos de autor sobre los mismos. Además, cuantos cambios deberán hacerse a un programa original para que pueda ser considerado un nuevo programa.

Sin embargo, junto con los reclamos respecto de las cada vez más elusivas modalidades de propiedad intelectual ha aparecido en la red una forma de libre circulación de información y conocimientos originados en los mismos usuarios. Se trata de los llamados wikis, documentos de hipertexto confeccionados en forma colectiva, de acceso libre para todas las personas que pueden interactuar en una página web, actualizándola y editándola en forma instantánea y democrática. Un buen ejemplo de ello es la Wikipedia, una enciclopedia online donde aportan millones de visitantes que contribuyen en forma libre y comunitaria a su contenido sobre una muy amplia variedad de temas, sin que sea necesario que el mismo sea revisado antes de ser aceptado para su publicación en la Web. Se publica en más de 100 idiomas y, en los principales, se puede acceder a más de 50000 artículos. La versión en inglés comenzó el 15 de enero de 2001[23]. Tres años y medio después, en septiembre de 2004, unos 10.000 editores activos trabajaban en 1.000.000 de artículos en más de 50 idiomas. En marzo de 2005 la versión inglesa seguía liderando el proyecto y superó el hito de 500.000 artículos, alcanzando el millón y medio entre todos los idiomas. Por su parte, la Wikipedia en castellano comenzó el 20 de mayo de 2001, y a día de hoy cuenta con 56357 artículos. Todos los días cientos de miles de visitantes de todo el mundo hacen decenas de miles de ediciones y crean miles de nuevos artículos.

Wikipedia es un proyecto de la fundación sin ánimo de lucro Wikimedia, así como lo son los siguientes proyectos plurilingües y de contenido libre:

[23] Sus fundadores fueron Jimmy Wales y Larry Sanger que se basaron en el concepto wiki. Wikipedia utiliza una plataforma de software wiki llamada MediaWiki, que permite a cualquier persona modificar una página en cualquier momento y poder ver los cambios instantáneamente (wiki significa «rápido» en hawaiano).

Wikcionario (Diccionario con sinónimos), Wikilibros (Libros de texto y manuales), Wikiquote (Colección de citas), Wikisource (Documentos originales), Wikiespecies (Directorio de especies), Wikinoticias (Noticias libres), Commons (Imágenes y multimedia), Meta-Wiki (Coordinación de proyectos). El principio que orientó a sus fundadores fue que el saber humano debería intercambiarse y fluir sin necesidad de permiso alguno.

Algunos critican la falta de control del material incorporado a la Wikipedia que puede ser errado, o malicioso, propagandístico o subversivo, en relación con los mismos principios que procura defender. Ya algunas medidas se han tomado que impiden la edición de conceptos cuestionados o que los corrigen rápidamente. Por otra parte, se espera que los colaboradores más fieles provean rápidamente a modificar las intervenciones que tengan un carácter doloso[24].

Otro caso muy exitoso de información compartida, derivado en forma impensada de la comunidad hacker es el sistema operativo Linux. Este sistema comenzó como un proyecto hacker del programador Linus Torvalds, quien lo creó como un clon del sistema operativo UNIX y lo colocó en Internet para que pudiera ser bajado en forma gratuita. Luego el programa fue objeto de muchas otras modificaciones por parte de usuarios.

Ejemplos recientes de información y conocimientos compartidos en Internet son los llamados Weblogs, conocidos como blogs, que son diarios online y los RSS (*Really Simple Syndication*)[25] que constituyen formatos diseñados para distribuir y compartir contenidos de la Web entre diversos sitios entre los cuales pueden mencionarse la BBC, CNET, CNN, Disney, Forbes, Motley Fool, Wired, Red Herring, Salon, Slashdot, ZDNet, y más, incluyendo los weblogs.

[24] "Desde esta perspectiva, el pensamiento es un proceso social, y no individual, y del mismo modo el conocimiento es un proceso de ampliación y revisión de la información, por parte de los comunes o de la inteligencia colectiva o general, que coopera en una sociedad-red". Como señaló Jimmy Wales "Todo es revisado por pares en tiempo real". Cf. http://en.wikipedia.org/wiki/Main Page o, en la versión en español, http://es.wikipedia.org/wiki/Portada.

[25] Inicialmente conocidos como *Rich Site Summary* y luego como *RDF Site Summary*.

El fenómeno de los blogs es sorprendente. Al principio aparecieron como una derivación de las páginas web personales, pero hoy trascienden el rol de diarios personales y pueden ser brazos de campañas políticas, programas de medios o de corporaciones. Pueden ser escritos por un autor ocasional o ser el resultado de colaboraciones de una comunidad. Cada segundo aparece uno nuevo y más de 80.000 se crean por día. El conjunto de blogs, muchos vinculados por enlaces, se denomina blogosfera y su tamaño parece estar duplicándose cada cinco meses y medio. En el mes de julio se habían identificado 14.2 millones de weblogs y más de 1.300 millones de enlaces[26].

Existe además mucho software muy utilizado que puede ser bajado gratuitamente desde la Web. Entre los programas más utilizados podemos mencionar: Winamp, Firefox, WinZip, Itunes, RealPlayer, Acrobat Reader. Existen además una multitud de software libremente accesible que tiende a proteger la privacidad y a evitar los virus cada vez más corrientes.

Todos estos nuevos desarrollos definen espacios de libertad y conocimientos compartidos en cierto modo incompatibles con la noción de propiedad individual pero ciertamente congruentes con el espíritu que se supone debería caracterizar Internet y el nuevo universo de la información y de las comunicaciones.

iv. Seguridad

Un aspecto relevante y relacionado con los anteriores es el referido a la seguridad cuyo principal componente es el referido a crímenes realizados mediante la utilización de computadoras. Por supuesto que, al referirnos a la seguridad, se apunta a un género de seguridad lógica que aparece amenazada en una época caracterizada por los virus y los hackers. De la interacción de unos con otros se han generado situaciones que abarcan una gama de hechos que van de lo claramente delictivo a lo moralmente cuestionable.

El robo por computadora no deja de ser robo y, como tal debe ser castigado. La incidencia de la sustracción de fondos y activos parece estar

[26] <http://www.technorati.com/weblog/blogosphere/index.html>

creciendo[27] y, con frecuencia, las empresas afectadas, en muchos casos bancos, no toman acciones contra los culpables, en caso de identificarlos, para no hacer público el hecho de que sus sistemas informáticos no son enteramente seguros.

También se han producido robos de información que pueden ser tanto o más dañinos que los anteriores. Han sido robados los datos de millones de usuarios de tarjetas de crédito. El crecimiento del e-commerce y del e-banking no deja de presentar dudas acerca de la información a la cual puedan eventualmente acceder quienes tengan conocimientos suficientes. Es también cierto que se han creado salvaguardias y existe software, incluso de acceso gratuito, para encriptar.

La ilusión de la privacidad y el anonimato en la Web es tan sólo eso: una ilusión. La actividad de los hackers parece no tener límites. Las nuevas salvaguardias que continuamente se están creando parecen constituir sólo interesantes desafíos para sus actividades. Un panorama de esto lo da el número de páginas web que están dedicadas a este tema. Ya no parece seguro darle un clic a cualquier enlace y, desde ya, en todo momento se enfatiza que hay que tener mucho, pero mucho cuidado, en abrir cualquier *attachment* que venga anexo a un correo que resulte sospechoso.

La última innovación en materia de actividad hacker parece estar dada por el llamado *phishing* que constituye un instrumento desarrollado para robar la identidad a través del e-mail. Su autor, bajo engaños, pretende que quien recibe un mail se vea engañado para revelar datos personales valiosos, como números de tarjetas de crédito, contraseñas, datos de cuentas bancarias. Para ello hace aparecer en los mails logos de apariencia legítima de organizaciones conocidas y otras informaciones identificatorias muchas veces tomadas de los sitios auténticos. Mediante un enlace suelen llevar a las incautas víctimas a un sitio falso (o un pop-up window) que luce exactamente como el sitio oficial. Y allí las víctimas del engaño pueden suministrar información personal a los perpetradores que la pueden utilizar para efectuar compras de bienes, para solicitar nuevas tarjetas o, en el peor de los casos, para robar la identidad.

[27] De George presentaba una estimación conservadora en 1999 de 3000 millones de dólares anuales.

Lamentablemente, encuestas realizadas entre adultos usuarios de Internet por el Annenberg Public Policy Center de la Universidad de Pennsylvania en general fallaron en el test que se les realizó respecto de sus conocimientos relativos a la privacidad en los sitios Web y a la posibilidad de identificar los *phishing* mails dolosos. Tampoco demostraron conocer las agencias que en los Estados Unidos ayudan a los consumidores a monitorear la posibilidad de robo de identidad.

Otro aspecto problemático de gran difusión es el referido a los programas *spyware* que buscan identificar los hábitos de los usuarios de la Web para mostrarles luego publicidad específica dirigida a sus intereses aparentes. Estos programas realizan un seguimiento del tráfico de Internet de ciertas personas, identificando qué servidores se visitan, qué archivos se bajan, qué compras se realizan, qué operaciones de home banking se llevan a cabo. Es decir, compilan un registro de las actividades que, de manera creciente, las personas realizan en la Web. Existen, por supuesto, programas *antispyware* pero, como los ardides de quienes espían evolucionan y se sofistican de modo constante, también es necesario mantener actualizados los programas que pretenden contrarrestarlos. También hace tiempo ya que existen las *cookies* que aparentemente no serían tan dañinas ya que son mensajes enviados del web server al web browser, que este guarda y que luego se utilizan para identificar usuarios y presentarles páginas web personalizadas de acuerdo con sus probables gustos.

En materia de actividad de los hackers otro desarrollo muy conocido es el referido a los virus que desparraman en la Web[28], no necesariamente con propósitos ilegales. ¿Pero qué es un hacker? En los medios y el conocimiento común se lo suele identificar como un criminal de la computación. En realidad, la mejor forma de caracterizarlo es como un experto en computación y programación que en forma no autorizada se introduce en un sistema de computación. Al comienzo de su historia se denominaba así al intruso en la computadora. Actualmente se pueden distinguir dos significados del término. El negativo, ampliamente aceptado por los medios y la población, relacionado con

[28] También los *worms* y los *Trojan horses*, que muchas veces son considerados también virus.

las actividades criminales. El segundo, aceptado por la comunidad de la computación que reconoce en el hacker un programador brillante o experto técnico y rechaza la connotación criminal para la cual ha encontrado las designaciones alternativas de "*cracke*r" o "*black hat*".

Muchos hackers no se ven como criminales y se consideran más bien exploradores y defensores de la libertad en el ciberespacio ya que pueden detectar los riesgos en la seguridad . En ciertos casos se los contrata para que descubran las debilidades de ciertos sistemas informáticos. Pero la evidencia reciente nos señala los muchos problemas que los virus y sus autores han creado a la creciente comunidad de usuarios no expertos en el tema. Y también en este caso se requiere la utilización de programas antivirus permanentemente actualizados.

v. Acceso y poder

La problemática del acceso a los sistemas informáticos se vincula con la cuestión del poder. El acceso a la información requiere del usuario cierto nivel mínimo de habilidades intelectuales: leer, escribir, razonar, calcular[29]. Estas habilidades se reciben en el sistema educativo formal. Pero además de ciertos niveles de competencia en lo que podría definirse como ***literacy*** y ***numeracy*** se hace necesario añadir una nueva habilidad básica de interacción con las nuevas tecnologías que ha sido denominada ***informacy***[30] A nivel individual será el acervo de tales habilidades el que determinará la posibilidad de acceder a ciertos niveles de conocimientos y control. Los conocimientos estarán acumulados en los distintos medios de información: bibliotecas, radios, televisión, teléfonos y, de manera creciente, en computadoras personales o en terminales conectadas por redes. Pero, la posibilidad de tener acceso a la información en sí misma está relacionada con la problemática de la propiedad arriba analizada.

Así la cuestión del acceso presenta dos facetas que definen dos umbrales de acceso. Uno individual dado por los niveles de conocimientos

[29] Lo que se denominaba formación básica en las tres **r:** lectu**r**a, escritu**r**a y a**r**itmética (en inglés **r**eading, w**r**iting, a**r**ithmetic).

[30] Cf. European Commission, **Living and Working in the Information Society: People First, Green Paper,** 1996.

necesarios para acceder a los nuevos sistemas de información. Y otro, global o nacional, que puede definirse por la brecha que experimentan quienes sólo tienen oportunidades limitadas de acceso a la tecnología, especialmente a Internet, en relación con los países más avanzados en ese aspecto. Es lo que se define como la brecha digital. En cierto sentido, parecería que la brecha, en lugar de ir cerrándose se fuera ensanchando y que los ricos fueran cada vez más ricos. Ello sería así, pues son los que tienen los medios y las oportunidades de tener acceso a la información y al conocimiento. Y un medio pensado para producir una creciente diseminación de ese conocimiento en forma igualitaria y democrática, parecería concentrarlo cada vez más. Y con el conocimiento se concentra el poder y con el poder también se concentra la riqueza.

Sin embargo, hay noticias que pueden despertar cierto grado de optimismo en esta cuestión. Si bien es cierto que la difusión del acceso a Internet no ha alcanzado los niveles que se esperaba, en buena medida por los costos que implicaría tener un equipo de computación y conectarse vía modem o por banda ancha, y aún por no tener posibilidades de conexiones eléctricas y telefónicas, ha surgido una alternativa bastante válida y que podría contribuir al achicamiento de la brecha. Son los teléfonos celulares.

El fenómeno adquiere especial relevancia en países africanos donde los teléfonos fijos son escasos, la electricidad muchas veces se corta, hay pocos aparatos de TV, las computadoras sólo pueden encontrarse en algunos ciber cafés de las principales ciudades. Pero los celulares se están difundiendo a una velocidad que supera en mucho a la de los países occidentales. De acuerdo con un estudio realizado con el apoyo de Vodafone, el gigante inglés de la telefonía celular, en Africa hay 82 millones de personas que utilizan teléfonos móviles sobre una población total de 700 millones[31]. En

[31] De acuerdo con las investigaciones realizadas en el Centre for Economic Policy Research de Londres con el apoyo de Vodafone, el 97% de la población de Tanzania utiliza celulares. En sólo 5 años el número de teléfonos celulares superó él de los teléfonos fijos, proceso que llevó 15 años a Gran Bretaña. Costa de Marfil ha sido uno de los primeros países africanos donde el número de celulares superó el número de teléfonos fijos. En Kenia en el 2002 había 770 mil celulares para una población de 3 millones. En el 2004 los celulares ya eran 1590800. En Nigeria la telefonía móvil crece a un 100% al año. Cf. Vodafone, "Africa: The Impact of Mobile Phones", **The Vodafone Policy Paper Series**, Nº 2, marzo 2005.

19 países africanos sobre cada 4 teléfonos 3 son celulares. En el estudio se muestra que en un país en vías de desarrollo un incremento de 10 celulares por cada 100 personas implicaría un incremento del PIB per capita de 0,59%. Además, de acuerdo con los resultados reseñados, tanto en Sudáfrica como en Egipto una considerable proporción de pequeñas empresas manifestaron que como consecuencia del uso de la telefonía celular sus beneficios habían aumentado, a pesar del mayor costo de las llamadas.

En realidad, todo parecería haber comenzado en Bangladesh donde a fines de los noventa el banco Grameen[32] organizó Grameen Telecommunications, una organización sin fines de lucro para proveer servicios de telefonía de bajo costo en zonas rurales. Con fondos del banco los entrepreneurs locales (95% de ellos mujeres) compraron teléfonos celulares para proveer sus servicios a los pobladores y ambos grupos obtuvieron considerables beneficios de índole diversa. El ejemplo cundió y se organizaron otros emprendimientos similares. Así la Grameen Foundation USA los organizó en Uganda y Rwanda.

Si se tiene en cuenta el creciente número de funciones que pueden estar cumpliendo hoy los teléfonos celulares (fotografía digital, mensajes de texto, agenda, computadora, reproductor de música, acceso a Internet) parecería que esta tecnología es la que irá eliminando la brecha digital. Sin embargo, hay países que parecen temer esos avances y la diseminación del conocimiento que ello implicaría. Así el gobierno chino pretende aislar la conexión local a Internet de la del resto del mundo pues, si bien quiere acceder a los beneficios comerciales que la conexión implica teme la posible influencia política negativa que entiende podría tener para la estabilidad del gobierno. Sin embargo, los llamados bloggers chinos han encontrado la forma de dar vuelta a las restricciones ubicando a sus blogs en un server fuera de China ofrecido por voluntarios de un programa denominado *"Adopt-a-Chinese Blog"*. De este modo el gobierno no los puede censurar.

[32] El Grameen Bank es una institución creada en Bangladesh por el economista Yunus para otorgar microcréditos para financiar microemprendimientos a pobladores muy pobres (los más pobres de entre los pobres). Bangladesh suele ser considerado hoy el caso de estudio para el impacto que la telefonía celular puede tener para las poblaciones más marginadas.

vi. Globalización y responsabilidad profesional

La evolución que se ha operado en el campo de la Etica de la Computación y la fusión de las tecnologías de la información con las de la comunicación, así como el creciente impacto de carácter global que estas tecnologías están teniendo ha llevado a muchos autores a preguntarse acerca de la naturaleza y alcance de las cuestiones que se discuten, algunas de la cuales fueron abordadas más arriba. De ese modo podría definirse de modo más preciso el campo de esta disciplina así como el nombre que mejor la definiría. Se ha propuesto el nombre *"Global Information Ethics"* para enfatizar el hecho de que los desarrollos tecnológicos más impactantes de las últimas décadas, Internet y la Web, tienen un carácter global y conectan a la gente en todo el mundo[33]. Otra propuesta es la de designarla como *"Information Communications Technology Ethics"* para resaltar la convergencia que, en el contexto globalizado, se ha ido produciendo en las cuestiones éticas relacionadas tanto con la información como con las comunicaciones[34]. A pesar de que no hay acuerdo sobre cambios en el nombre, o aun sobre si es necesario producirlos, se acepta el hecho de que Internet y la Web han tenido un impacto significativo sobre el carácter y el dominio de esta disciplina.

De acuerdo con Deborah Johnson con la tecnología de Internet han surgido nuevas cuestiones no existentes en la era pre-Internet[35]. Ellas se refieren al **alcance** global e interactivo que tiene Internet, a la posibilidad de poder comunicarse en **forma anónima[36]** y de **reproducir** la información en el medio. Estas características implicarían una diferencia moral ya que el comportamiento en una red electrónica será moralmente diferente del aquel que se llevaría a cabo fuera de ese medio. Destaquemos nuevamente que Johnson entiende que las cuestiones éticas que plantea Internet son distintas

---

[33] Cf. Bynum, T. W., and S. Rogerson, "Global Information Ethics: Introduction and Overview", **Science and Engineering Ethics**, Vol. 2, Nº 2, 1996.

[34] Cf . van den Hoven, J., Introna, L.C., Johnson, D.J. and Nissenbaum, H., "Editorial", **Ethics and Information Technology**, Vol. 1, Nº 1, 1999.

[35] Cf. Johnson, D. J., ""Ethics Online", **Communications of ACM**, Vol. 40, Nº 1, enero 1997.

[36] Dentro de límites cada vez más acotados como se ha visto.

pero no nuevas. Otros autores, que fueron analizados en un anterior trabajo[37], piensan en cambio que las cuestiones éticas suscitadas por Internet son nuevas y requieren un campo de estudio separado.

Sin embargo, sin pretender profundizar demasiado en este tema, resulta claro que la globalización vinculada a Internet parecería requerir de normas de carácter también global que establezcan patrones de comportamiento y comporten una defensa global de valores humanos. Esta es por cierto una tarea complicada pues haría necesaria la promulgación de leyes de carácter también global que muchos países y gobiernos no parecerían aún estar en disposición de aceptar fácilmente, tal como el caso de China arriba reseñado, parecería indicar. Sin embargo, tal como también se indicó, parecería difícil imponer barreras a algo que parece tener la fuerza y el empuje para superar todo tipo de obstáculos. También deberían terminar siendo globales normas que procuren proteger la privacidad, la propiedad y el acceso sin que ello implique dar vía libre a comportamientos criminales y faltos de ética.

Dentro de este contexto y como una respuesta a la necesidad de fijar estándares para guiar a los usuarios en una utilización ética de las computadoras, parece pertinente mencionar la propuesta realizada por el *Computer Ethics Institute* referida a lo que denomina "Los diez mandamientos de la ética de la computación"[38], que se detallan a continuación:

1. No utilizarás una computadora para dañar a otros.
2. No interferirás con el trabajo de computación de otros.
3. No espiarás en los archivos de la computadora de otros.
4. No utilizarás una computadora para robar.
5. No utilizarás una computadora para levantar falso testimonio.

[37] Cf. Montuschi, L., "Aspectos éticos de las tecnologías de la información y de la comunicación: la ética de la computación, Internet y la World Wide Web", **Serie Documentos de Trabajo de la UCEMA**, Nº 298, agosto de 2005.

[38] Cf. <www.brook.edu/its/cei/overview/Ten_Commanments_of_Computer_Ethics.htm>

6. No copiarás ni utilizarás software de propiedad privada sin haber pagado por el mismo.
7. No utilizarás los recursos de computación de otra persona sin autorización o compensación adecuada.
8. No te apropiarás del producto intelectual de otros.
9. Pensarás acerca de las consecuencias sociales del software que estás escribiendo o del sistema que desarrollas.
10. Utilizarás siempre la computadora de modo tal que asegure consideración y respeto por tus congéneres.

A pesar de que se entiende que estos mandamientos han sido elaborados como un punto de partida válido para formular reglas que puedan ser aceptadas con un consenso bastante generalizado, los mismos han generado también cierta dosis de perplejidad. Por un lado, debe destacarse que no cubren todas las cuestiones éticas que se plantean en la *Computer Ethics*. Las principales cuestiones que se cubrirían, de modo muy parcial, serían las de propiedad, seguridad y privacidad. Y no debería inferirse que, por el hecho de observar tales mandamientos, un usuario estaría necesariamente actuando de manera ética[39]. Nuevas cuestiones están surgiendo de manera continua. Tampoco debería concluirse que alguien que en algún momento viole lo dispuesto por alguno de estos mandamientos estaría actuando necesariamente de modo no ético[40]. Por otra parte, como se ha señalado, algunos de estos mandamientos parecen ser triviales y otros, en cambio, apuntan a cuestiones muy importantes. Con todas las críticas que se han formulado[41] se debería, no obstante, considerar la observancia de los mismos

[39] Restringir el daño posible sólo a las personas, como lo indica el 1º, es muy limitado. Sería claramente falto de ética utilizar las computadoras para dañar al medio ambiente o a los animales.

[40] Así, por ejemplo, se menciona en el 3º que no se deberán espiar los archivos de la computadora de otros pero no se considera el caso de que "el otro" puede estar cometiendo algún tipo de crimen y el espionaje podría evitar daños y peligros para la mayoría de la población, como sería el caso del terrorismo.

[41] Cf.Fairweather, N.B., "Commentary on theTen Commandments for Computer Ethics" <www.ccsr.cse.dmu.ac.uk/resources/professionalism/codes/cei_command_com.html>

como un válido punto de partida para un comportamiento ético en relación con el uso de la computación.

El carácter universal y globalizado de las nuevas tecnologías de la información, en particular Internet y la World Wide Web, constituye un obstáculo no desdeñable para la implementación de normas de responsabilidad profesional. Otra dificultad adicional está dada por el hecho de que la utilización de estas tecnologías no está limitada a profesionales específicos. Por consiguiente, si bien resulta muy plausible que organizaciones profesionales como la Association for Computing Machinery (ACM) de los Estados Unidos reconozcan la existencia de responsabilidades profesionales para sus miembros, que han plasmado en un código de ética que incluye referencias a "imperativos morales generales" y a "responsabilidades profesionales", el efecto de estas normas será necesariamente limitado, tanto al ámbito geográfico de aplicación como al universo de usuarios. Además, debe tenerse presente que la responsabilidad no puede limitarse al uso que se haga de las tecnologías, sino que la misma debería ser extendida a la creación de los sistemas informáticos.

El mundo ha ingresado a una nueva era dominada por avances tecnológicos impensados hasta hace pocas décadas. Estos desarrollos están creando nuevas formas de organización de la sociedad, nuevas formas de vida y de interrelación entre las personas. Individuos y organizaciones públicas y privadas se están volviendo crecientemente dependientes de la tecnología de la computación. Pero, el paso de una era a otra aún no totalmente definida no está exento de problemas y de dilemas éticos. En este trabajo se han analizado algunas de las principales cuestiones éticas generadas por el avance de la tecnología informática. Pero debe aceptarse que, con los nuevos y continuos desarrollos, nuevas cuestiones éticas problemáticas se habrán de presentar que requerirán actitudes positivas de individuos y gobiernos para preservar los valores sociales y éticos que constituyen los fundamentos de las distintas culturas.

REFERENCIAS BIBLIOGRAFICAS

Bellinger, G., Castro, D. y Mills, A., "Data, Information, Knowledge and Wisdom", www.outsights.com/systems/dikw/dikw.htm,1997.

Boatright, J.R., **Ethics and the Conduct of Business,** Prentice Hall, 2003.

Boulding, K., "Notes on the Information Concept", **Explorations,** (Toronto), 6, 1955.

Bynum, T. W., and S. Rogerson, "Global Information Ethics: Introduction and Overview", **Science and Engineering Ethics**, Vol. 2, Nº 2, 1996.

Bynum, Terrell Ward, "Computer Ethics: Basic Concepts and Historical Overview", **The Stanford Encyclopedia of Philosophy** (Winter 2001 Edition), Edward N. Zalta (ed.),
De George, R.T., **Business Ethics,** Prentice Hall, 1999.

European Commission, **Living and Working in the Information Society: People First, Green Paper,** 1996.

Fairweather, N.B., "Commentary on theTen Commandments for Computer Ethics" <ccsr.cse.dmu.ac.uk/resources/professionalism/codes/cei_command_com>

Hartman, Laura P., "Technology and ethics: privacy in the workplace", **Business and Society Review**, vol. 106 (no. 1), 2001.

Johnson, D. J., ""Ethics Online", **Communications of ACM**, Vol. 40, Nº 1, enero 1997.

Kock, N.F., Jr., McQueen, R.J. y Corner, J.L., "The Nature of Data, Information and Knowledge Exchanges in Business Processes: Implications for Process Improvement and Organizational Learning", **The Learning Organization**, Vol.4, Nº 2, 1997.

Langlois, R. y Garrouste, P., "Cognition, Redundancy, and Learning in Organizations", trabajo presentado a la **Conference on Evolutionary Economics and Technological Change**, 6-8 octubre 1994, Estrasburgo, Francia.

Machlup, F., "Semantic Quirks in Studies of Information", en Machlup F. Y Mansfield U., (Eds.), **The Study of Information**, **Interdisciplinary Messages**, New York, John Wiley,1983.

Marx, G.T. y Sherizen, S., "Monitoring On The Job: How to Protect Privacy as Well as Property", **Technology Review**, Noviembre-Diciembre 1986.

Montuschi, L., "Datos, información y conocimiento. De la sociedad de la información a la sociedad del conocimiento", **Serie Documentos de Trabajo de la Universidad del CEMA,** Nº , 192, julio 2001.

Montuschi, L., "El conocimiento tácito y el conocimiento codificado en la economía basada en el conocimiento", **Anales de la Academia Nacional de Ciencias Económicas**,Vol. XLVII, Buenos Aires, 2002.

Montuschi, L., "Aspectos éticos de las tecnologías de la información y de la comunicación: la ética de la computación, Internet y la World Wide Web", **Serie Documentos de Trabajo de la UCEMA**, Nº 298, agosto de 2005.

Parent, W.A., "Privacy, Morality and the Law", **Philosophy and Public Affairs**, Vol. 12, 1983.

Schoderbek, C.G., Schoderbek, P.P. y Kefalas, A.G., **Management Systems. Conceptual Considerations**, Business Publications, Dallas, 1990.

Tavani, H.T. y Moor, J.H., "Privacy Protection, Control of Information, and Privacy-Enhancing Technologies", **Computers and Society**, Vol.. 31,Nº 1, 2001.

URL = <http://plato.stanford.edu/archives/win2001/entries/ethics-computer/>.

van den Hoven, J., Introna, L.C., Johnson, D.J. and Nissenbaum, H., "Editorial", **Ethics and Information Technology**, Vol. 1, Nº 1, 1999.

Vodafone, "Africa: The Impact of Mobile Phones", **The Vodafone Policy Paper Series**, Nº 2, marzo 2005.