PROGRAMA DEL DIPLOMADO DE PROCESO BENCHMARKING.

TEMA 8. PRIVACIDAD Y SEGURIDAD DE LOS DATOS:

OBJETIVO:
Ésta unidad comprenderá el estudio de la necesidad en que las empresas fabricantes de CRM coinciden con la responsabilidad de cómo se utilizan la privacidad y seguridad de los datos tomados de los clientes, así cómo la de éstos para proporcionarlos.

8.1.- PRIVACIDAD Y SEGURIDAD DE LOS DATOS:

Todas las empresas fabricantes de CRM coinciden en que la responsabilidad de cómo se utilizan los datos tomados de los clientes es de las empresas que usan las soluciones.
Quien mantiene una base de datos debe hacer todos los esfuerzos para que sus empleados cumplan con las adecuadas medidas de seguridad y confidencialidad, y denuncien cualquier violación de la misma. El respeto en el uso y la no vulnerabilidad de la información de los clientes es la piedra fundamental para una relación exitosa con ellos.
Datos como el nombre, el domicilio, la dirección de mail, el número de teléfono, no necesariamente son datos secretos ni confidenciales. Pero si esos mismos datos son tomados en conjunto o procesados para inferir características, tendencias o perfiles de sus titulares, bien podrían constituir información confidencial y sensible. Por lo tanto, todo dato no considerado personalísimo y/o sensible es plausible de ser utilizado comercialmente dentro de un marco ético.

8.2.- CONSIDERACIONES LEGALES:

Obvio es decir que Internet es una red global y básicamente insegura, tanto a nivel de arquitectura y tecnología de red, como de los grandes productos software que sirven para comunicarse en ella, la protección de datos no cumple a priori requisitos minimamente aceptables de pura protección tecnológica de los datos que por ella circulan. Esa inseguridad de la red es también difícil de solucionar, toda vez que de nuevo la única gran potencia está interesada en la interceptación sistemática de todas las comunicaciones que circulan por la Red, a través de Échelon y Carnivore, y casi con toda seguridad, las grandes multinacionales que controlan los productos básicos para navegar por la Red, como Microsoft, persiguen propósitos similares.
En este caso, está claro que a la citada empresa le conviene la identificación de los usuarios de sus programas en la Red, lo que le da un importante control sobre las copias ilegales de su propio software y le permite reforzar su política empresarial, que a todas luces está encaminada a controlar al máximo, con fines comerciales, el tráfico que se produce en la Red.

Los agentes principales:

En el ámbito público el gran coloso americano y, en la esfera privada, el monopolista del software de base para PC y de las grandes suites ofimáticas; pero junto a ellos hay multitud de operadores interesados en un control más o menos intenso de la información, y por lo tanto de los datos personales, que circulan por Internet. Por lo que se refiere a los grandes operadores privados, Microsoft cambia su plan de servicios “Web” por el miedo de las empresas a ceder su lista de clientes. El subtítulo es: La firma de Bill Gates corrige la estrategia de MyServices, que centralizaba los datos del ínter nauta para que pudiera usar y comprar servicios desde cualquier máquina sin registrarse de nuevo, ante la resistencia de los suministradores. Evidentemente MyServices no era sino un pretexto para que Microsoft se hiciera con los datos de clientes de miles y miles de empresas, lo que repugna a los principios más elementales de la protección de datos personales.

En esta situación de interesada anarquía de protección de datos en la Red, no es extraño que proliferen los intentos destinados a rebajar al máximo la protección de la
Intimidad en la red, a veces incluso con perspectivas doctrinalmente “diabólicas”, como
las que tienden a considerar a Internet como medio de comunicación; es de suponer que para buscar el pretexto de integrar toda la red en el régimen excepcional, en relación con la protección de la intimidad, de los mass media, que está reconocido, incluso, y de forma muy razonable -para los auténticos medios de comunicación, no para Internet- en la Directiva 95/46. Lo “diabólico” consistiría en entender que Internet está sometido a la legislación especial de los mass media, más centrada en la libertad de información, que en la intimidad de las personas, con lo que quedaría justificada la actual situación de desprotección de esta última

La Internet la World Wide Web:

Debe entenderse como una realidad en si misma, independiente de su contenido y de la utilidad que se obtenga del mismo, por lo que en ningún caso podría tener la consideración apriorística
de un medio de comunicación como son la prensa radio y televisión. No obstante, cuando Internet o la WWW se utilicen como instrumento para ofrecer al público este tipo de servicios de comunicación pública, la cosa cambia; pero en todo caso el medio de comunicación sigue siendo el contenido y no el continente; es decir, “los contenidos”, nunca la red, ni siquiera cuando es La Red.
A través del tratamiento automatizado de los datos obtenidos, que incluye la posibilidad de cotejo con más datos procedentes de otras fuentes, como los formularios on- line es posible la elaboración de un patrón de conducta detallado de los afectados, o lo que es lo mismo, su perfil personal, cuya obtención es vista con extremo recelo por cualquier legislación seria de protección de datos personales. Todo ello es posible a través del empleo de técnicas de datamining o minería de datos.

8.2.1.- ACUMULACION DE INFORMACIÓN INNECESARIA:

Este es, precisamente uno de los fenómenos más preocupantes relacionados con las técnicas de datamining y que está en directa relación con el control difuso de las personas, que puede acabar resultando letal para las libertades, en la sociedad de la información.

Pensemos, por ejemplo, en lo que pueden significar los sistemas de espionaje global Echelon y Carnivore, a los que más adelante se hará referencia, que rompen el Derecho Fundamental no ya sólo a la intimidad de las personas, sino al secreto de las comunicaciones y con un alcance global. Hoy las cosas son más sutiles y mucho más peligrosas también. En todo caso, lo mismo que hace el mundo anglosajón con las comunicaciones mundiales, pueden hacerlo los grandes actores de la sociedad de la información, normalmente en menor escala y con otros móviles; pero si no se actúa con firmeza contra tales actividades, el riesgo para la libertad de comunicaciones, la intimidad de las personas y las libertades mismas a escala global, es mucho más que una amenaza.
El almacenamiento sistemático de datos para su posterior minería, es posible en razón de su bajo costo, combinado con su extrema utilidad, que para las empresas se traduce en la posibilidad de elaborar perfiles personales, para explotarlos en función de sus intereses. En general es demasiado frecuente que se soliciten abusivamente todo tipo de datos personales para obtener cualquier servicio o adquirir cualquier producto. Estos datos pueden ir desde la simple -o no tan simple- dirección de correo electrónico, hasta una completa descripción conteniendo nombre, dirección, ingresos, aficiones, etc.
Cómo puede tomarse en serio la legislación nacional de protección de datos personales, cuando se está tolerando que una anarquía casi absoluta reine en Internet en esta materia. Eso, a largo plazo, va a dar lugar a una deslegitimación de los organismos nacionales de protección en Europa y de la propia legislación Europea, que puede resultar “vencida” por la tozuda dinámica de los hechos, que se está produciendo en Internet.

8.2.2.- LEGISLACIONES:

El anonimato en Internet como garantía de la Intimidad:
Recomendación 3/97, de 3 de diciembre de 1997, del Grupo del Artículo 29.
La idea de fondo de la Recomendación es que ha de procurarse que, en la medida de lo posible, los rastros creados al utilizar Internet no permitan identificar al usuario. En todo caso este deseo no es mucho más que eso, si la Unión Europea no decide tomar medidas concretas, pues ya se ha dicho que al instalar Windows, o los programas más usuales de Microsoft, lo primero que piden es la identificación como usuario legal, que luego es transparente, por ejemplo, en los documentos generados por MS-Word y que acaba reflejándose en las cookies. Se

trata de un auténtico “mundo al revés”, habida cuenta de que en mecanismos de comunicación más tradicionales, como el correo postal, la expresión del remitente no es obligatoria. Lo mismo sucede en el mundo de las telecomunicaciones, cuando la Directiva 97/66, obliga a que se puedan desactivar de forma sencilla la identificación de llamadas, u obliga a la cancelación de datos de facturación, una vez pasado el plazo legal de impugnación de la misma.
Lo anterior implica que debiera ser posible, e incluso la configuración por defecto del correspondiente software, mantener el anonimato a la hora de enviar correo electrónico, navegar por la Web y adquirir la mayor parte de bienes y servicios a través de Internet. Eventualmente pueden ser necesarios algunos controles de los particulares
que envían colaboraciones a foros, grupos de debate, etc.; pero la práctica directa de identificación de las personas resulta muy a menudo desproporcionada, por lo que habría que impulsar otras soluciones. Las restricciones legales que puedan imponer los Gobiernos al derecho de mantener el anonimato o a los medios técnicos utilizados al efecto, deberán en todo momento ser proporcionadas y limitarse a lo estrictamente necesario para proteger un interés general específico en una sociedad democrática, como está claramente establecido en el artículo 8 de la Convención Europea de 1950, para los Derechos Humanos y las Libertades Fundamentales.
Tecnologías Avanzadas de Privacidad (PET): Posición común adoptada en la 23 Reunión del IWG en Hong Kong, el 15 de abril de 1998.

La posición común de la tecnología:

1) La tecnología por si misma nunca podrá ser la solución para garantizar la intimidad en la Web. Se necesita además un marco regulatorio (legislación, códigos de conducta, contratos, auditorias independientes y recursos legales para el individuo).
2) Cualquier usuario debería tener la opción de visitar una Web de forma anónima. Este precepto debería aplicarse incluso en las descargas de información de dominio público. En este último caso, la información personal únicamente podría ser procesada mientras el usuario se encuentre leyendo información de la Web, excepto para las conexiones de datos, que lo será en la medida necesaria para los propósitos de seguridad.
3) Se requerirá el consentimiento previo e informado del afectado como paso previo al tratamiento de sus datos personales. Más aún, los datos personales no deberán transmitirse de forma automática hacia una Web sin una previa notificación al afectado, quien deberá tener siempre la opción de bloquear dicha transmisión.
4) Por lo que se refiere a los motores de búsqueda, se dan las siguientes soluciones:

- Restringir que los motores realicen búsquedas de datos personales, lo que sería difícil de implementar y poco práctico.
- Impedir la recopilación de datos de los usuarios de los buscadores. Lo que es enormemente importante, para evitar la elaboración de los siempre indeseables perfiles personales.

Abundando en lo anterior, se trataría, como es lógico, de que no se pudiera recopilar datos personales sin el consentimiento informado de los afectados.

Los motores de búsqueda:

Podrían permitir que las personas que introduzcan datos personales en su página Web inserten, a su vez, un código que informe al buscador que no desean que dichos datos sean tratados, lo que contra diría la teoría de que existe un consentimiento tácito al tratamiento de los datos personales por un motor de búsqueda, por el mero hecho de colocar los datos en Internet. En todo caso, lo que es seguro que no se permite es otro tipo de tratamientos. Informar al usuario del motor de búsqueda de sus derechos y obligaciones y del uso que se va a hacer de los registros de sus búsquedas; y, por supuesto, pedirle consentimiento para todo ello.
Opinión sobre Plataforma de Preferencias de Privacidad (P3P) y norma de perfiles abierta (OPS): Dictamen 1/1998, de 16 de junio de 1998, del Grupo del Artículo 29.

Se trata de la opinión manifestada por el Grupo, en su reunión de 16 de junio de 1998, en relación con las denominadas plataformas de preferencias de privacidad (P3P), que conciben la posibilidad de que pueda procederse al tratamiento de los datos en virtud de un acuerdo entre el usuario de Internet y el sitio Internet en que se registran los mismos. Se trata de mundializar un sistema de inspiración USA, cuyo mayor problema es su bajo nivel de protección de la intimidad. Preocupa el hecho de que las reglas que configuran este proyecto son las que se pretenden aprobar en el seno del consorcio World Wide Web. E1 P3P es una iniciativa del W3C cuyo objetivo es elaborar un protocolo mediante el cual, usuario y Web negocian las preferencias relativas a la privacidad, pudiendo el usuario decidir si acepta los términos de la Web antes de navegar a través de ella. Véase http://www.w3.org/P3/Overview.html.

El gran problema, como apunta muy bien el Grupo, es que se va al mínimo de protección, que está muy lejos de ser el vigente en la Unión Europea. Como dice el propio Grupo, una plataforma técnica para la protección de la intimidad no bastará por sí sola para proteger la intimidad personal en la Red. Es necesario aplicarla en un contexto de normas de protección de datos que sean ejecutables y deparen a todas las
Personas un nivel mínimo y no negociable de protección de la intimidad. Recurrir a la P3P y a la OPS sin que exista tal marco jurídico presenta el riesgo de pasar la responsabilidad básicamente al usuario necesitado de protegerse, una evolución que minaría el principio sentado internacionalmente de que el cumplimiento de los principios de la protección de datos incumbe al “controlador de datos”.
(Directrices OCDE 1980, Convenio del Consejo de Europa nº 108 de 1981, Directrices NNUU1990, Directivas comunitarias 95/46/CE y 97/66/CE).
Tal inversión de responsabilidades también presupone un nivel de conocimientos sobre los riesgos que el tratamiento de datos entraña para la intimidad de las

personas, algo que no resulta realista esperar de la mayoría de los ciudadanos. Es más, habría que añadir que la gente ni siquiera suele modificar en el navegador la posición "por defecto" sobre las preferencias de privacidad, que al ser mínima, daría lugar, de ordinario, a un nivel de protección igualmente mínimo.
Existe el riesgo de que la P3P, una vez puesta en práctica en la próxima generación de software de navegación, pueda llevar a los operadores radicados en la UE a creer erróneamente que podrían quedar eximidos de algunas de sus obligaciones legales. Por tanto, el software de navegación vendido o distribuido en la UE debe estar concebido y configurado de tal manera que resulten imposibles los acuerdos en línea contrarios a la legislación vigente en materia de protección de datos. A lo expresado por el Grupo, he de añadir que aquí es, precisamente, donde está la gran responsabilidad de la UE, que es no transigir frente a nadie, por importante y poderoso que sea, en la defensa de sus propios puntos de vista, que son, precisamente, los adecuados para que la persona humana tenga Derechos Fundamentales de calidad, sobre todo en cuanto al respeto de la vida privada. El Grupo es consciente de ello, y por lo tanto, entre las Instituciones de la UE, no se ignora dónde está el problema, que no se solucionará hasta que el gigante comercial tenga una política más adecuada a sus propios intereses y menos a los intereses de alguno de nuestros aliados, sobre todo cuando están muy lejos de coincidir con los propios de la UE.

8.3.- Requisitos del software y hardware en Internet:

Recomendación 1/99, de 23 de febrero de 1999, adoptada por el Grupo del Artículo 29 de la Directiva 95/46

Esta Recomendación 1/99 atiende al hecho, ya reseñado, de que se pueden obtener multitud de datos personales del afectado, a través, fundamentalmente, del software, y a veces incluso del hardware que emplea durante la navegación por Internet, por lo que
hace las siguientes recomendaciones, dirigidas, sobre todo, a la industria informática:

1.- Hay que acatar el principio de consentimiento informado, por lo que la insta a trabajar en productos que respeten la vida privada y se ajusten a la normativa europea en materia de protección de datos.
2. Los productos Internet (hardware y software) debieran permitir al interesado decidir libremente en cuanto al tratamiento de sus datos personales, ofreciéndole instrumento de fácil manejo para filtrar (es decir rechazar o modificar) la recepción, el almacenamiento o el envío de la información persistente del cliente según unos criterios determinados (incluidos los perfiles, el dominio o la identidad del servidor Internet, el tipo y duración de la información recopilada, almacenada o enviada y así sucesivamente).

Esto supone que: El software navegador debería proporcionar opciones para que el usuario pueda configurar el mismo, especificando el tipo de información que debería o no debería recopilar y transmitir.

Eso supone que la configuración por defecto, debiera ser restrictiva. En el caso de las cookies, el usuario debería contar siempre con la opción de aceptar o rechazar el envío o almacenamiento de un cookie en su totalidad. A eso debo añadir, que en ningún caso debieran permitirse “amenazas” del tipo que si no aceptas el cookie, no visualizarás la página, o la persistencia de nuevas cookies, hasta el hastío del ínter nauta, de forma parecida a lo que hacen los bancos con las comisiones, que obligan al desvalido cliente, a “pelear” su retroacción, comisión a comisión y euro a euro hasta que se aburra, que es de lo que ostensiblemente se trata. Una actitud tan proclive al abuso no debiera poder considerarse seriamente legal.

Entiendo, además, que en principio no debieran requerirse datos de carácter personal, para el acceso a información que no fuese imprescindible; por ejemplo, información “de pago”. Como mínimo debiera existir una causa justificada.

8.4.- ENFOQUE COMUNITARIO INTEGRADO DE LA PROTECCIÓN DE DATOS EN LÍNEA:

Consideraciones del Grupo sobre Echelon y Carnivore. El Grupo considera este tema, a colación, con carácter general, de las actividades de “husmeo de la red”, actividades que a menudo son pura y simplemente delictivas, como el husmeo de secuencias que suelen emplear los números de tarjetas de crédito. Según el Grupo, cuyas consideraciones reproduzco textualmente, cuando el husmeo se realiza en nudos o empalmes centrales de Internet, esto permitiría interceptar y controlar a gran escala el contenido de mensajes de correo electrónico y los datos sobre tráfico de acuerdo con determinadas características, principalmente la presencia de palabras clave. Como actividad de control general y exploratoria, el husmeo sólo puede permitirse si se respetan las condiciones establecidas en el artículo 8 del Convenio Europeo de Derechos Humanos, aun cuando lo lleven a cabo organismos gubernamentales.

En este contexto, resulta interesante señalar las preocupaciones actuales existentes en todo el mundo sobre un posible

8.4.1 Control de las comunicaciones internacionales:

El sistema de interceptación de satélites "Echelon". La supervisión internacional es actualmente una cuestión candente en el programa de trabajo del Parlamento Europeo. En un informe dirigido al Director General de Estudios del Parlamento Europeo sobre el desarrollo de las tecnologías de supervisión y el riesgo de abuso de la información económica, se menciona que el sistema "Echelon" ha existido durante más de veinte años.

De acuerdo con este informe, Echelon utiliza intensamente las redes mundiales de comunicación de la NSA y el GCHQ similares a Internet para permitir que centros remotos de información interroguen a ordenadores en cada sitio dedicado a la

recopilación y reciban los resultados de forma automática. Otro sistema de control polémico es Carnivore que, de acuerdo con la información publicada por el EPIC (Centro de Información sobre la Intimidad Electrónica), controla el tráfico en las instalaciones de los proveedores de servicios de Internet con objeto de interceptar información de criminales sospechosos en el correo electrónico. El EPIC afirma que Carnivore podría analizar millones de mensajes de correo electrónico por segundo y permitir a los agentes encargados de velar por el cumplimiento de la ley interceptar todas las comunicaciones digitales de un cliente de un proveedor de servicios de Internet. El Congreso de Estados Unidos, los medios de comunicación y la comunidad de defensa de la denominada “privacidad” han planteado preguntas muy serias sobre la legalidad de Carnivore y los abusos que puede conllevar su uso.

En respuesta a las protestas públicas relacionadas con Carnivore, el 27 de julio de 2000 la Fiscal General Janet Reno anunció que se permitiría el acceso de un "grupo de expertos" a las especificaciones técnicas del sistema, con objeto de aliviar la preocupación pública. El debate sobre la vigilancia mundial de las comunicaciones también forma parte del programa de trabajo del Consejo de Europa. El 27 de abril de 2000, el Comité de expertos en delitos del ciberespacio publicó su "proyecto de Convenio sobre delincuencia en el ciberespacio". Este Convenio obligaría a las empresas que ofrecen servicios de Internet a recoger y almacenar datos destinados a los organismos públicos encargados de velar por el cumplimiento de la ley, con lo que facilitaría la recopilación de información. Habría que apostillar que eso significa que también se ocupan de interceptar y no de todo lo contrario.

Sería necesario un intercambio de tales datos entre autoridades gubernamentales de distintos países, incluso los que no son parte en el Convenio Europeo de Derechos Humanos u otros instrumentos del Consejo de Europa o de la UE en materia de protección de datos. Hasta la fecha, no se ha previsto ningún requisito sustancial para proteger el derecho fundamental a la intimidad y la protección de los datos personales en terceros países que reciben datos de carácter personal sobre ciudadanos de la UE, y tampoco se han establecido los principios básicos para respetar las normas relativas a derechos humanos fundamentales como la necesidad y la proporcionalidad. De hecho, dice el propio Grupo que en una declaración realizada en abril de 2000, durante la Conferencia de Estocolmo, en la que señalaron con preocupación que, según las propuestas presentadas, los proveedores de servicios de Internet deberían almacenar habitualmente los datos sobre tráfico no sólo con fines de facturación, con objeto de permitir un posible acceso de los organismos encargados de velar por el cumplimiento de la ley.

8.4.2.- La Conferencia:

Señaló que esta retención constituiría una invasión ilegal de los derechos fundamentales que garantiza el artículo 8 del Convenio Europeo de Derechos Humanos y declaró que en los casos específicos en que se hayan de conservar datos sobre tráfico, debería existir una necesidad demostrable, el período de

conservación debería ser lo más breve posible y la práctica debería estar claramente regulada por la ley. El propio Grupo Recuerda que en su Recomendación 2/99, el Grupo de Trabajo del artículo 29 ha tratado los aspectos que afectan a la intimidad en la interceptación de las comunicaciones. En esta Recomendación, el Grupo de Trabajo señala que cualquier interceptación de las telecomunicaciones, definida como el conocimiento por un tercero de los datos sobre el contenido y el tráfico de las telecomunicaciones privadas entre dos o más corresponsales y, en especial, de los datos sobre tráfico relacionados con la utilización de servicios de telecomunicación, constituye una violación del derecho individual a la vida privada y a la confidencialidad de la correspondencia. De esto se desprende que las interceptaciones son inaceptables, a menos que cumplan tres criterios fundamentales, de conformidad con lo dispuesto en el apartado 2 del artículo 8 del Convenio Europeo para la Protección de los Derechos Humanos y las Libertades Fundamentales del 4 de noviembre de 1950 y de la interpretación que el Tribunal Europeo de Derechos Humanos ha hecho de esta disposición: un fundamento jurídico, la necesidad de la medida en una sociedad democrática y la conformidad con alguno de los objetivos legítimos enumerados del Convenio .

8.5.- Etiqueta de "privacidad":
Un supuesto de autorregulación en la Red.

Según precisa el Grupo, esta etiqueta de respeto a la vida privada se configura como un sello de calidad que se impone a un sitio Web. A lo largo de los años han aparecido diversas etiquetas, entre las que destacan las de Truste, Privaseek, Better Business Bureau y WebTrust. Algunas de estas organizaciones estadounidenses opera en el ámbito internacional, incluida Europa; otras aspiran a hacerlo. Al mismo tiempo, en Europa están surgiendo iniciativas similares con fines internacionales, por ejemplo Labelsite en Francia. Las etiquetas se otorgan a las empresas que cumplen una serie de requisitos especificados por el organismo que las concede, que puede ejercer algún tipo de control sobre el cumplimiento de las políticas de privacidad de las empresas que las poseen mediante revisiones periódicas de sus actividades. En algunos casos, el organismo que concede la etiqueta se encarga también de las quejas presentadas contra empresas que tienen la etiqueta en sus sitios Web. La denominada etiqueta de "privacidad" plantea, según el Grupo, una serie de cuestiones:
La primera se refiere al contenido de la etiqueta. El derecho a la información y al acceso, el principio de minimización de datos, el derecho a oponerse, el principio de legitimidad y proporcionalidad y la obligación de notificar a la autoridad nacional de protección de datos son algunas de las piedras angulares de los principios europeos de protección de datos. El principal riesgo social sería la difusión de etiquetas de privacidad en toda Europa, lo que confundiría a los usuarios y a los responsables del tratamiento. Aunque pueden dar esta impresión, no todas las etiquetas garantizan seriamente todos los principios de protección de datos mencionados.

El segundo problema radica en el control de las prácticas de “privacidad” de los sitios Web. Se pueden practicar numerosos tipos de control. Algunas de las principales preocupaciones al respecto son:
¿Quién tiene el control?
¿Cómo lo ejerce?
¿Con qué clase de mandato otorgado por la empresa controlada?
En el peor de los casos, parece que el responsable del tratamiento será, principalmente, el propio interesado, con todos los problemas que esto conlleva a la hora de identificar los fallos en la observación de las prácticas de privacidad declaradas, demostrarlos y notificarlos a la empresa que asigna las etiquetas. Además, no todos los organismos que conceden etiquetas pueden garantizar que las empresas actúen según pretenden sus políticas.

¿Quién pagará? Dado que la asignación de etiquetas es una iniciativa privada que a menudo no cuenta con apoyo económico gubernamental, algunos organismos que conceden etiquetas sufrirán la presión de las empresas a las que supuestamente controlan.
¿Qué sanciones se impondrán, si se impone alguna? Según sigue diciendo el Grupo, que en general se me antoja demasiado escéptico para con la autorregulación, no se deben tampoco subestimar los posibles efectos de las etiquetas de “privacidad” en la protección de ésta, pues pueden ayudar a concienciar a los usuarios de Internet sobre la misma. El Grupo llega a propugnar una normativa europea sobre tales etiquetas, controles de auditoria y otras medidas, sin darse cuenta de que se insertan en el marco de la autorregulación, previsto en la propia Directiva 95/46, bajo el nombre de “Códigos de Conducta”, que pueden funcionar perfectamente, como se ha demostrado en España con el Código de Conducta de la AECE (Asociación Española de Comercio Electrónico), que se ha centrado, sobre todo, en la autorregulación del envío de publicidad a través de la Red. Este Código Tipo, que es como se denomina en España a los Códigos de Conducta en esta materia, ha sido inscrito en la Agencia de Protección de Datos de España, y muchas respuestas al escepticismo del Grupo del Artículo 29, puesto que en el Código ético, aparte de las importantes empresas de todos los sectores, que forman parte de la AECE, han participado tres de las principales asociaciones de consumidores, así como la Asociación para el Autocontrol de la Publicidad.
Asimismo es de indicar que de los 10 miembros que integran el Comité de Protección de Datos de la AECE, órgano que tiene atribuida la competencia de control del cumplimiento del Código ético, 4 son representantes de asociaciones de consumidores y 1 de la Asociación de Autocontrol de la Publicidad. Aparte de respetarse al máximo los principios de protección de datos personales, el Código ético no deja de incluir sanciones, entre las que se comprenden la advertencia, la amonestación y la retirada temporal o definitiva del sello de garantía, así como la propuesta de expulsión de la Asociación, e incluso la posibilidad de publicitar la sanción impuesta.

8.6.- Otras Cuestiones a Destacar:

Según reconoce el propio Grupo, la recopilación de información relativa al usuario en entornos en línea es una práctica de importancia económica y estratégica. En concreto cita unas líneas, extraídas de una famosa publicación americana, que ilustran esta idea: Son demasiadas las empresas, incluidas muchas compañías punteras que están surgiendo en Internet, que no se han centrado lo suficiente en el valor de los perfiles de los clientes. Quien posea los derechos sobre los perfiles de los clientes en línea será quien determine los ganadores y los perdedores de esta nueva era. Además, las listas de clientes se venden o comparten, principalmente a través de la fusión de compañías de tecnología de la información que de este modo aumentan la cantidad de datos y perfiles a su disposición.
Es de destacar, asimismo, que la Directiva 97/66, sobre protección de la intimidad y de los datos personales, en el ámbito de las telecomunicaciones, establece que los equipos -lo que sin duda incluye a las herramientas de Internet- deberán incorporar los mecanismos necesarios para proteger la intimidad de los usuarios. Esta prevención, sencillamente no se cumple y lo cierto es que no se exige su cumplimiento, sencillamente porque no se quiere. Bastaría con exigir a los "productos de Internet" respeto por la normativa europea, para poder vender en Europa.

Aparte de las Directivas 95/46 y 97/66, el Grupo cita otras reglamentaciones comunitarias que tratan algunos aspectos relacionados con Internet. Cabe mencionar los siguientes instrumentos: la Directiva 1999/93/CE de 13 de diciembre por la que se establece un marco comunitario para la firma electrónica, la Directiva 97/7/CE de 20 de mayo de 1997 relativa a la protección de los consumidores en materia de contratos a distancia y la Directiva 2000/31/CE de 8 de junio de 2000 relativa a determinados aspectos jurídicos de los servicios de la sociedad de la información (Directiva sobre el comercio electrónico). A ello vamos a referirnos a continuación.

8.6.1.- VIDA PRIVADA, COMERCIO ELECTRÓNICO y FIRMA DIGITAL:

En el marco del comercio electrónico, cobra especial importancia la seguridad de sistemas de información y los aspectos técnicos, en general, para evitar que las tan frecuentes tentaciones de cometer fraudes informáticos en la red tengan un peligro real
para las transacciones económicas que se producen en la misma. Al principio de este trabajo, ya me había referido a las conexiones seguras tipo SSL, sistemas de firma digital, intranet u otras redes seguras del tipo VPN, etc.
Además existen sistemas de dinero electrónico que preservan el anonimato de las compras en Internet. El dinero electrónico, en general se basa en sistemas de firma digital complejos, donde el dinero va "firmado" por la entidad financiera correspondiente y no por el usuario, con la particularidad de que puede "gastarse" por el propio usuario, sin dejar rastro de la persona que ha incurrido en el correspondiente expendio.
Es más anónimo, incluso, que el dinero de papel. Su gran problema es que no parece que haya existido gran interés en su comercialización, aparte también de otra posible problemática de blanqueo de dinero, aunque en este tema me parece

que se magnifica el pretexto frente al problema, puesto que a los titulares de los medios de pago en la red, que no en vano son grandes corporaciones, no están interesados en el anonimato de las transacciones, sino en todo lo contrario. Veamos algunos supuestos relacionados con el comercio electrónico, en relación con la vida privada.

8.6.2.- Las transferencias electrónicas de fondos:

El principal problema, en relación con la protección de datos personales, que se puede generar como consecuencia de la irrupción de la contratación electrónica es el relacionado con las transferencias de fondos que se efectúan a través de la red para el abono de la contraprestación de los bienes y servicios adquiridos. En este caso, el problema surge como consecuencia del hecho de que gran parte de esas transferencias se realizan por medio de tarjetas de crédito, lo que supone una revelación, a través de un medio inseguro como Internet, de una serie de circunstancias que pueden ser conocidas por terceros, que incluso suplanten al consumidor que ha revelado dichos datos. Es más, a partir de los datos de pagos por Internet, se puede generar un auténtica almacenamiento de datos relacionados con las aficiones y costumbres de consumo del titular de la tarjeta, para someterlos a posteriores operaciones de datamining, que puede dar lugar, con toda facilidad, a la obtención de perfiles personales, e incluso a su comercialización por el prestador. Las soluciones son de dos tipos. Por una parte cabe establecer medios que aseguren el anonimato del gasto efectuado y, por otra, se puede garantizar que el tratamiento efectuado por el proveedor del medio de pago y por el acreedor se ajuste íntegramente a los principios reguladores de la protección de datos. Sobre este punto, hay que tener en cuenta la Recomendación R (90) 19, de13 de septiembre de 1990, adoptada por el Comité de Ministros del Consejo de Europa.

8.6.3.- Utilización del Dinero Electrónico:

Recomendación 1/97, del Grupo del Artículo 29. La recomendación considera que el comercio electrónico a través de Internet, en principio habría de ajustarse al modelo establecido para los pagos fuera de línea. Los particulares debieran poder elegir entre distintos medios de pago seguros, inclusive los que permiten mantener el anonimato, como alguna variante ya comentada de dinero electrónico. En todo caso sería ya hora de desechar las inseguras tarjetas de banda magnética, y sustituirlas por las denominadas tarjetas inteligentes o tarjetas-chip, que son incomparablemente más seguras. Cabe que la tarjeta lleve incorporados más mecanismos de seguridad, incluso claves criptográficas, lo que reduciría enormemente los riesgos en caso de pérdida.
Recomendación R (90) 19, de 13 de septiembre de 1990, del Consejo de Europa, sobre protección de datos de carácter personal utilizados con fines de pago. La idea fuerza de la Recomendación es que el interesado no debiera verse jamás

obligado a utilizar un medio de pago electrónico, ya que si no lo hace, sin duda se reduce en mucho el trasiego de datos de carácter personal, que se producen durante las transacciones. La gran pregunta es: ¿es ello factible? al menos en términos realistas y operativos. Personalmente pienso que no. Lo que habría que hacer es impulsar las transacciones con dinero electrónico anónimo y, si se considera que hay un incremento de los riesgos de blanqueo, hacer lo que realmente hay que hacer y parece que se intenta evitar a toda costa: algo tan sencillo como aplicar la legislación de protección de datos personales, aunque moleste a importantes empresas transnacionales y a poderosos aliados.

8.6.4.- La Recomendación del Consejo de Europa:

Contiene prevenciones sobre extremos como los siguientes: Recogida y grabación de los datos, que debe cumplir los siguientes requisitos:
- El organismo proveedor del medio de pago solamente podrá recoger los datos que sean necesarios para poner a disposición el medio de pago y los servicios relacionados con su utilización, incluso con fines de control.
- Los datos sólo deberían recogerse del propio afectado, y cuando ello no sea posible, habría que informarle de las fuentes que se pueden consultar y de las consecuencias que pueden resultar de una negativa a ello o de una posterior revocación del consentimiento.
- El beneficiario solamente podría recoger datos de carácter personal con fines de verificación de la identidad del titular, del medio de pago y de la determinación de la validez o del carácter lícito de la operación de pago, u otra operación análoga.
- Cuando se realice una operación con ayuda de un medio de pago, los datos personales relacionados con dicha operación sólo deberían ser recogidos y registrados por el organismo proveedor de los medios de pago únicamente en la medida en que sean necesarios para la validez y para la prueba de la operación, así como para la realización de los servicios y el cumplimiento de toda obligación derivada del derecho interno relacionada con su utilización.

En términos semejantes a la Directiva 97/66, se establece que el operador de la red de comunicaciones debería poder, recoger y registrar únicamente los datos de carácter personal necesarios para la ejecución, la prueba y la facturación de los servicios que suministra:

- Utilización de los datos. Lo básico es que no procede llevar a cabo la interconexión de las diferentes utilizaciones del medio de pago por el individuo
- Cesión de datos. Procede en términos similares a los generales de las Directivas europeas sobre Protección de Datos.
- Derechos de acceso y de rectificación. Sin duda los tiene el afectado que, previa petición, puede obtener de forma comprensible todos los datos referidos a ella, incluso los que figuran en un medio de pago y solicitar, en su caso, la rectificación de los mismos.

8.6.5.- La Protección de Datos Personales en Internet:

Está condicionada por el carácter básicamente inseguro de La Red, así como por su calidad de red global. La inseguridad técnica de los niveles básicos de Internet propicia los abusos en la captación de datos personales, en el que están interesadas importantes empresas multinacionales, que son precisamente las que han de desarrollar los productos hardware y software que permiten operar en Internet. Asimismo Estados de gran peso específico tienen interés en controlar la información que circula por Internet, y de hecho lo hacen. Poner límites a este tipo de prácticas es difícil debido al carácter global de La Red y a la interesada anarquía que propicia su nada inocente desregulación, que la somete, más todavía, a la ley de los fuertes.

La enorme disparidad de Ordenamientos en materia de Protección de Datos Personales y, sobre todo, los planteamientos tan divergentes, entre la normativa europea y la norteamericana, así como la permisividad que ésta tiene para los intereses empresariales, dificultan hasta el extremo la consecución de unos estándares mínimos razonables, de protección de datos personales en Internet. Es obvio, en estas circunstancias, que para que la Unión Europea pueda hacer respetar sus puntos de vista sobre protección de la vida privada en Internet, ha de mantenerlos con firmeza. Se trata de algo tan sencillo como de atreverse a aplicar la propia legislación, incluso si esto supone dejar claro que determinados productos y formas de hacer negocio de importantes empresas transnacionales están, en Europa, al margen de la Ley. De no actuar así se va a producir, a medio plazo, una deslegitimación de los organismos nacionales de protección de datos en Europa y de la propia legislación Europea, que puede resultar “vencida” por la tozuda dinámica de los hechos, que se está produciendo en Internet.