ÉTICA LEGISLACIÓN Y PROFESIÓN

MARCOS SÁNCHEZ-ÉLEZ
GRADO EN INGENIERÍA INFORMÁTICA
2015-2016

BASADO EN LAS TRANSPARENCIAS DE LA PROFESORA SARA ROMAN NAVARRO

LEYES

DEFINICIÓN DE LEY

- **RAE: ley (Del lat. *lex, legis)***
  - Precepto dictado por la autoridad competente, en que se manda o prohíbe algo en consonancia con la justicia y para el bien de los gobernados.
  - En el régimen constitucional, disposición votada por las Cortes y sancionada por el jefe del Estado.
- **Wikipedia: ley**
  - Es una norma jurídica dictada por el legislador, es decir, por la autoridad competente, en el que se manda o prohíbe algo en consonancia con la justicia cuyo incumplimiento conlleva a una sanción

DEFINICIÓN DE LEY
LEY NATURAL

- **Es una doctrina ética y jurídica que defiende la existencia de derechos del hombre fundados o determinados en la naturaleza humana, universales, anteriores y superiores (o independientes) al Derecho tal como le conocemos**
  - Conocida desde Platón y Aristóteles y formulada por Santo Tomás de Aquino
- **Si estos principios no son recogidos o proscriptos por el ordenamiento jurídico éste no puede considerarse un verdadero ordenamiento jurídico**

DEFINICIÓN DE LEY
LEY NATURAL

- **Según algunos autores unos ejemplos de la ley natural serían:**
  - Libertad
  - Autodefensa
  - Propiedad

¿Estáis de acuerdo?

DEFINICIÓN DE LEY
LEY "CONVENCIONAL"

- **Es un sistema creado por los humanos, normalmente en deliberaciones públicas**

- **Características (fuente Wikipedia):**

  - Generalidad: La ley comprende a todos aquellos que se encuentran en las condiciones previstas por ella, sin excepciones de ninguna clase.
  - Obligatoriedad: por una parte establece obligaciones o deberes jurídicos y por la otra otorga derechos. Su incumplimiento da lugar a una sanción, a un castigo impuesto por ella misma.
  - Permanencia: Se dictan con carácter indefinido.
  - Abstracta e impersonal
  - '*Se reputa conocida:* Nadie puede invocar su desconocimiento o ignorancia
  - Irretroactiva: Como norma general, regula los hechos que ocurren a partir de su publicación, hacia lo futuro.

DEFINICIÓN DE LEY

- **El propósito de la ley (FA Fagothey (1959)) :**
  - El ignorante necesita instrucción y control por el sabio
  - La sanción es necesaria para la seguridad de la sociedad
  - La acción concertada exige trabajo en equipo y liderazgo
  - La sociedad debe cumplir las nuevas condiciones armoniosamente

¿Estáis de acuerdo?

¿Se cumplen cuando el parlamento sanciona una ley?

DEFINICIÓN DE LEY
TIPOS DE LEYES

- **Ley fundamental:**
  - Es la que establece principios por los que deberá regirse la legislación de un país; suele denominarse Constitución.
- **Ley orgánica:**
  - Cuando nace como consecuencia de un mandato constitucional para la regulación de una materia específica.
  - Según el art. 81 de la Constitución, “son las L.O. las relativas al desarrollo de los derechos fundamentales y de las libertades públicas las que aprueban los estatutos de autonomía y el régimen electoral general, y las demás previstas en la Constitución”. La L.O. formalmente no es otra cosa, que una ley reforzada, dotada de una mayor rigidez que la ordinaria.
- **Ley ordinaria:**
  - Las leyes ordinarias son el instrumento norma de realización de la función legislativa por parte de las Cortes y pueden referirse a cualquier materia que no esté reservada por la constitución a otro tipo de norma

EL PROCEDIMIENTO LEGISLATIVO

Fuente: Asociación de Periodistas Parlamentarios

- **PROYECTOS DE LEY**

1. **APROBACIÓN**. Los proyectos de ley se aprueban por el Consejo de Ministros y se remiten al Congreso de los Diputados acompañados de una Exposición de Motivos y de los antecedentes necesarios para pronunciarse sobre ellos (art. 88 CE).
2. **ENMIENDAS**. La Mesa del Congreso recibe el texto y ordena su publicación en el BOCG y el envío a la Comisión correspondiente. A partir de la fecha de publicación, los Grupos Parlamentarios disponen de 15 DÍAS para presentar ENMIENDAS al texto (De Totalidad o al Articulado).
3. **DEBATE DE TOTALIDAD**. En caso de presentarse enmiendas de totalidad, su debate en el Pleno es el primer trámite que tiene que salvar el proyecto de ley (art. 112 RC).
4. **PONENCIA**. Concluido el plazo de enmiendas la Comisión correspondiente designa, de entre sus miembros, una PONENCIA, grupo reducido de diputados representantes de todos los Grupos Parlamentarios que, a puerta cerrada, redactan un INFORME (art. 113 RC).
5. **DELIBERACIÓN EN COMISION**. Concluido el Informe de la Ponencia, la Comisión se reúne de nuevo para debatirlo, así como las enmiendas artículo por artículo. Tras votarlos, emite un DICTAMEN que someterá al Pleno de la Cámara.
6. **DELIBERACIÓN EN PLENO**. Que puede comenzar con un nuevo turno de defensa por parte del Gobierno y de presentación del Dictamen por un miembro de la Comisión (art. 118 RC).
7. **TRAMITACIÓN EN EL SENADO**. Recibido el texto, el Senado dispone de DOS MESES para tramitar el proyecto, plazo en el que sus posibilidades de actuación son tres:
    - Aprobar el texto, Introducir enmiendas o Interponer un veto

EL PROCEDIMIENTO LEGISLATIVO

Fuente: Asociación de Periodistas Parlamentarios

- **PROPOSICIONES DE LEY DE INICIATIVA PARLAMENTARIA.**
  - Del Congreso. Puede presentarlas un diputado con la firma de otros catorce o un GP con la sola firma de su portavoz (art. 126.1 RC).
  - Del Senado. Puede presentarlas un Grupo Parlamentario o 25 senadores (art. 108.1 RS).
  - Remisión al Gobierno. Tras calificarla, la Mesa respectiva ordena su publicación y remisión al Gobierno para que manifieste su criterio y su conformidad o no si supone aumento o disminución de créditos presupuestarios (art. 126.2 RC/ 151 RS).
  - La toma en consideración es un debate similar al de totalidad de los proyectos de ley. Se produce cuando los Grupos autores de la proposición deciden, de acuerdo con el cupo de que disponen, su inclusión en el Pleno.
  - Después el trámite es idéntico al de los proyectos de ley.

EL PROCEDIMIENTO LEGISLATIVO

- **PROPOSICIONES DE LEY DE INICIATIVA POPULAR**
  - En esta misma línea, la Constitución prevé, también, la participación directa de los ciudadanos en el proceso de producción normativa, configurando al pueblo, mediante la presentación de 500.000 firmas, como sujeto de la iniciativa legislativa […].
  - La puesta en marcha del procedimiento exige que la Comisión Promotora presente ante la Mesa de la Cámara un texto articulado dotado de unidad sustantiva precedido de una exposición de motivos. Para evitar gastos y esfuerzos inútiles la Mesa realizará un examen de admisibilidad […]
  - Una vez admitida la proposición, se inicia el procedimiento de recogida de firmas, […]; y también se podrán recoger las firmas por vía electrónica siempre que se garantice la voluntad auténtica del ciudadano que suscribe la iniciativa legislativa popular. (AÑADIDO 2006)
  - Recogidas las firmas exigidas, se inicia la tramitación parlamentaria. […]

EL PROFESIONAL DEBE CONOCER LAS LEYES QUE AFECTAN A SU PROFESIÓN

¿QUÉ LEYES NOS AFECTAN?

CÓDIGO PENAL

DELITOS INFORMÁTICOS

COPYRIGTH, CANON DIGITAL, PATENTES DE SOFTWARE …

LEY DE PROPIEDAD INTELECTUAL

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

LEY ORGÁNICA DE PROTECCIÓN DE DATOS

LEY DE SERVICIOS DE LA SOCIEDAD DE LA INFORMACIÓN Y DE COMERCIO ELECTRÓNICO

DELITOS INFORMÁTICOS

Cada equipo busca información sobre:

- Código penal (sin entrar en delitos de copyrigtht) - 2 equipos
- Ley Torquemada + otras leyes de ciberseguridad - 2 equipos
- Instituto Nacional de Ciberseguridad INCIBE
- Hackers vs Crackers
- Qué no es delito y debería serlo
- CNI - NSA y otras agencias de inteligencia

(+ Debate formal sobre hackers y crackers)

LEY DE PROPIEDAD INTELECTUAL

Todos los equipos trabajan sobre el mismo tema pero aportando distintos puntos de vista:

- Opinión sobre la LPI según el rol asignado
- Preguntas sobre la ley y su rol
- SW Libre y licencias cc (por el profesor)
- Caso práctico, qué licencia tiene el TFG por defecto, ¿se puede cambiar? ¿Y el código generado?¿Quién es el autor intelectual del trabajo?

LEY ORGÁNICA DE PROTECCIÓN DE DATOS

Cada equipo busca información sobre:

- Derechos básicos
- Obligaciones (2 equipos)
- Tratamiento de ficheros
- Cloud Computing
- Tecnología RFID
- Redes Sociales
- Video Vigilancia

LEY DE SERVICIOS DE LA SOCIEDAD DE LA INFORMACIÓN Y DE COMERCIO ELECTRÓNICO

Alguna vez tendréis que leer una ley (son 32 hojas):

- Exposición de motivos
- Título I
- Título II
- Título III y IV
- Título V y VI
- Título VII (dos equipos)
- Anexo

BASADO EN LAS TRANSPARENCIAS DE LA PROFESORA SARA ROMAN NAVARRO

DELITOS INFORMÁTICOS

TIPOS DE DELITOS

- **Un delito es aquella acción (conducta activa) u omisión (no hacer, conducta pasiva) que realiza una persona, que puede ser calificada como dolosa (intencionada) o imprudente y que es sancionada por la ley.**
  - Los delitos se clasifican en graves, menos graves y leves o faltas en función de la pena con la que son sancionados.
  - Son delitos graves aquellos a los que la Ley castiga con pena de prisión superior a 5 años
  - Los delitos menos graves son los sancionados con pena de prisión de 3 meses a 5 años
  - Faltas son infracciones castigadas con penas leves

DEFINICIÓN: DELITOS INFORMÁTICOS

- **Conductas de intrusismo informático:**

"Comportamientos de acceso o interferencia no autorizados, de forma subrepticia, a un sistema informático o red de comunicación electrónica de datos y utilización de los mismos sin autorización o más allá de lo autorizado" (Esther Morón)

DEFINICIÓN: DELITOS INFORMÁTICOS

“Todo ilícito penal llevado a cabo a través de medios informáticos y que está íntimamente ligado a los bienes jurídicos relacionados con las tecnologías de la información o que tiene como fin estos bienes.”

http://www.delitosinformaticos.com/delitos/codigopenal.shtml

“Todas aquellas acciones u omisiones típicas, antijurídicas y dolosas, trátese de hechos aislados o de una serie de ellos, cometidos contra personas naturales o jurídicas, realizadas en uso de un sistema de tratamiento de información y destinadas a producir un perjuicio en la víctima a través de atentados a la sana técnica informática, lo cual, generalmente, producirá de manera colateral lesiones a distintos valores jurídicos, reportándose, muchas veces, un beneficio ilícito en el agente, sea o no de carácter patrimonial, actúe con o sin ánimo de lucro” **(Marcel Huerta y Claudio Líbano)**

DEFINICIÓN: DELITOS INFORMÁTICOS

- **Los equipos informáticos como nuevos bienes jurídicos: integridad de la información y del propio equipo (HW y SW).**

- **Aparte de los bienes jurídicos tradicionales, que pueden ser accedidos y vulnerados por medios informáticos: patrimonio, intimidad, identidad, material con copyright …**

TIPOS DE DELITOS INFORMÁTICOS

- **Delitos contra la intimidad: descubrimiento y revelación de secretos: arts. 197.1 y 197.2 CP**
- **Utilización abusiva de equipos terminales de telecomunicaciones: art. 256 CP**
- **Delitos de daños, con especial referencia al sabotaje informático: art. 264.2 CP**
- **Delitos contra el material con copyright: art. 270**
- **Delitos relativos al mercado y a los consumidores: art. 278.1 CP**

CÓDIGO PENAL ESPAÑOL

- **Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal.**
  - Vigencia desde 24 de Mayo de 1996
  - Hay una revisión de Junio de 2010
  - Esta revisión vigente desde 17 de Enero de 2013 (http://noticias.juridicas.com/base_datos/Penal/lo10-1995.html)
- **Tipos de delitos comunes y "clásicos" tipificados**
- **No existe un Título específico relacionado con delitos informáticos**

CÓDIGO PENAL ESPAÑOL

TÍTULO X. Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio: CAPÍTULO PRIMERO. Del descubrimiento y revelación de secretos

Artículo 197

- El que, para descubrir los secretos o vulnerar la intimidad de otro, sin su consentimiento, se apodere de sus papeles, cartas, **mensajes de correo electrónico** o cualesquiera otros documentos o efectos personales **o intercepte sus telecomunicaciones o utilice artificios técnicos de escucha, transmisión, grabación o reproducción del sonido o de la imagen, o de cualquier otra señal de comunicación**, será castigado con las penas de prisión de uno a cuatro años y multa de doce a veinticuatro meses.
- Las mismas penas se impondrán al que, sin estar autorizado, se apodere, utilice o modifique, en perjuicio de tercero, **datos reservados de carácter personal o familiar de otro que se hallen registrados en ficheros o soportes informáticos, electrónicos o telemáticos**, o en cualquier otro tipo de archivo o registro público o privado. Iguales penas se impondrán a quien, sin estar autorizado, acceda por cualquier medio a los mismos y a quien los altere o utilice en perjuicio del titular de los datos o de un tercero.

CÓDIGO PENAL ESPAÑOL

TÍTULO XIII. Delitos contra el patrimonio y contra el orden socioeconómico, Capítulo VI de la defraudaciones: Sección 3 de las defraudaciones del fluído eléctrico y análogas

Artículo 256

- El que hiciere uso de cualquier **equipo terminal de telecomunicación**, sin consentimiento de su titular, ocasionando a éste un perjuicio superior a 400 euros, será castigado con la pena de multa de tres a 12 meses.

CÓDIGO PENAL ESPAÑOL

TÍTULO XIII. Delitos contra el patrimonio y contra el orden socioeconómico

- En el marco de los denominados delitos informáticos, […], relativa a los ataques contra los sistemas de información, se ha resuelto incardinar las conductas punibles en dos apartados diferentes, al tratarse de bienes jurídicos diversos.
  - El primero, relativo a los daños, donde quedarían incluidas las consistentes en dañar, deteriorar, alterar, suprimir o hacer inaccesibles datos o programas informáticos ajenos, así como obstaculizar o interrumpir el funcionamiento de un sistema informático ajeno.
  - El segundo apartado se refiere al descubrimiento y revelación de secretos, donde estaría comprendido el acceso sin autorización vulnerando las medidas de seguridad a datos o programas informáticos contenidos en un sistema o en parte del mismo

CÓDIGO PENAL ESPAÑOL

TÍTULO XIII. Delitos contra el patrimonio y contra el orden socioeconómico:
CAPÍTULO IX. De los daños

Artículo 264

- El que por cualquier medio, **sin autorización y de manera grave borrase, dañase, deteriorase, alterase, suprimiese, o hiciese inaccesibles datos, programas informáticos o documentos electrónicos ajenos**, cuando el resultado producido fuera grave, será castigado con la pena de prisión de seis meses a dos años.
- El que por cualquier medio, **sin estar autorizado y de manera grave obstaculizara o interrumpiera el funcionamiento de un sistema informático ajeno, introduciendo, transmitiendo, dañando, borrando, deteriorando, alterando, suprimiendo o haciendo inaccesibles datos informáticos**, cuando el resultado producido fuera grave, será castigado, con la pena de prisión de seis meses a tres años.
- Se impondrán las penas superiores en grado a las respectivamente señaladas en los dos apartados anteriores y, en todo caso, la pena de multa del tanto al décuplo del perjuicio ocasionado, cuando en las conductas descritas concurra alguna de las siguientes circunstancias:

  1.º Se hubiese cometido en el marco de una organización criminal.

  2.º Haya ocasionado daños de especial gravedad o afectado a los intereses generales.

CÓDIGO PENAL ESPAÑOL

TÍTULO VII. De la trata de seres humanos

Artículo 197

- El que por cualquier medio o procedimiento y vulnerando las medidas de seguridad establecidas para impedirlo, acceda sin autorización a datos o programas informáticos contenidos en un sistema informático o en parte del mismo **o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo**, será castigado con pena de prisión de seis meses a dos años.

Artículo 248

- Cometen estafa los que, con ánimo de lucro, utilizaren engaño bastante para producir error en otro, induciéndolo a realizar un acto de disposición en perjuicio propio o ajeno.
- También se consideran reos de estafa:
  - Los que fabricaren, introdujeren, poseyeren o facilitaren **programas informáticos específicamente destinados a la comisión de las estafas** previstas en este artículo

CÓDIGO PENAL ESPAÑOL

CAPÍTULO XI. De los delitos relativos a la propiedad intelectual e industrial, al mercado y a los consumidores: SECCIÓN 1. De los delitos relativos a la propiedad intelectual

Artículo 270

- Será castigado con la pena de prisión de seis meses a dos años y multa de 12 a 24 meses quien, con ánimo de lucro y en perjuicio de tercero, reproduzca, plagie, distribuya o comunique públicamente, en todo o en parte, una obra literaria, artística o científica, o su transformación, interpretación o ejecución artística fijada en cualquier tipo de soporte o comunicada a través de cualquier medio, sin la autorización de los titulares de los correspondientes derechos de propiedad intelectual o de sus cesionarios.
- No obstante, en los casos de distribución al por menor, atendidas las características del culpable y la reducida cuantía del beneficio económico, siempre que no concurra ninguna de las circunstancias del artículo siguiente, el Juez podrá imponer la pena de multa de tres a seis meses o trabajos en beneficio de la comunidad de treinta y uno a sesenta días. En los mismos supuestos, cuando el beneficio no exceda de 400 euros, se castigará el hecho como falta del artículo 623.5.

CÓDIGO PENAL ESPAÑOL

CAPÍTULO XI. De los delitos relativos a la propiedad intelectual e industrial, al mercado y a los consumidores: SECCIÓN 3. De los delitos relativos al mercado y a los consumidores

Artículo 278

- El que, para descubrir un secreto de empresa se apoderare por cualquier medio de datos, documentos escritos **o electrónicos, soportes informáticos** u otros objetos que se refieran al mismo, o empleare alguno de los medios o instrumentos señalados en el apartado 1 del artículo 197, será castigado con la pena de prisión de dos a cuatro años y multa de doce a veinticuatro meses.
- Se impondrá la pena de prisión de tres a cinco años y multa de doce a veinticuatro meses si se difundieren, revelaren o cedieren a terceros los secretos descubiertos.
- Lo dispuesto en el presente artículo se entenderá sin perjuicio de las penas que pudieran corresponder **por el apoderamiento o destrucción de los soportes informáticos.**

HACKERS

HISTORIA

- **1970. Con la aparición de ARPANET se abre la veda para controlar un computador desde otro computador**
- **1983. Aparece la película "Juegos de Guerra", se cree que esta película popularizó el fenómeno hacker.**
- **1980-1990. Se producen los primeros ataques orquestados por el Club 414 de San Francisco, los ataques se realizaron desde la Universidad de Stanford*.**
  - Estas actividades hicieron que en EEUU apareciera la primera ley que daba jurisdicción al servicio secreto sobre "el fraude en los computadores"
- **1984. Aparece la publicación "2600: The Hacker Quarterly", más tarde aparece Phrack**
- **1988. Aparece la primera noticia relacionada con un incidente hacker cuando un estudiante de la Universidad de Cornell consigue infectar a 6000 PCs y dejarles sin internet durante 2 días***
- **1990. Se crea Electronic Frontier Foundation**
- **1995. Primer arrestado por el FBI, Kevin Mitnick por robar numeros de tarjetas de crédito**
- **2000. Se producen una gran cantidad de ataques, "Mellisa", "Love Bug", "Killer Resume" …**

*Denning PJ (1990) Computers under attack: intruders, worms and viruses. ACM Press, New York

HISTORIA

- **Los ejemplos anteriores como otros tantos que se pueden encontrar en libros de texto o por la web equiparan el termino Hacker con el de Pirata Informático**
- **Si preguntáramos a personas fuera del mundo de las TICs equipararían el termino Hacker con el de criminal**

DELITOS INFORMÁTICOS

¿ESTÁ BIEN UTILIZADO EL TÉRMINO HACKER?

HACKER

- A person who enjoys exploring the details of programmable systems and how to stretch their capabilities, as opposed to most users, who prefer to learn only the minimum necessary.
- One who programs enthusiastically (even obsessively) or who enjoys programming rather than just theorizing about programming
- A person capable of appreciating hack value
- A person who is good at programming quickly
- An expert at a particular program, or one who frequently does work using it or on it; as in `a Unix hacker'. (Definitions 1 through 5 are correlated, and people who fit them congregate)
- An expert or enthusiast of any kind. One might be an astronomy hacker, for example
- One who enjoys the intellectual challenge of creatively overcoming or circumventing limitations
- [deprecated] A malicious meddler who tries to discover sensitive information by poking around. Hence `password hacker', `network hacker'. The correct term for this sense is cracker.

CRAKER

- **One who breaks security on a system.**
  - Coined ca. 1985 by hackers in defense against journalistic misuse of hacker (q.v., sense 8). An earlier attempt to establish `worm' in this sense around 1981-82 on Usenet was largely a failure.
  - Use of both these neologisms reflects a strong revulsion against the theft and vandalism perpetrated by cracking rings.
    - While it is expected that any real hacker will have done some playful cracking and knows many of the basic techniques, anyone past larval stage is expected to have outgrown the desire to do so except for immediate, benign, practical reasons (for example, if it's necessary to get around some security in order to get some work done).
    - Thus, there is far less overlap between hackerdom and crackerdom than the mundane reader misled by sensationalistic journalism might expect.
  - Crackers tend to gather in small, tight-knit, very secretive groups that have little overlap with the huge, open poly-culture this lexicon describes; though crackers often like to describe *themselves* as hackers, most true hackers consider them a separate and lower form of life.

ÉTICA HACKER

- The belief that information-sharing is a powerful positive good, and that it is an ethical duty of hackers to share their expertise by writing open-source and facilitating access to information and to computing resources wherever possible.
- The belief that system-cracking for fun and exploration is ethically OK as long as the cracker commits no theft, vandalism, or breach of confidentiality.

ÉTICA HACKER

- **Todos los hacker comparten *technical tricks*, software y (cuando es posible) recursos computacionales**
  - Es posible funcionar sin un control central, si no cooperativamente como en Usenet, FidoNet e Internet (Internet address)
- **Podríamos decir que todos los hacker comparten el principio de código abierto y muchos además el de SW libre**
- **Es mas controvertido el punto asociado a si craquear un sistema es ético**

ÉTICA HACKER

Según Levy (1984) todos los hackers comparten los siguientes principios éticos

- Acceso libre a los computadores y otros recursos TIC (cualquier cosa que pueda enseñarte como funciona el mundo debería ser ilimitada y total)
- Toda la información debería ser libre
- No es necesario un gobierno centralizado
- Los hackers deben ser juzgados por sus obras
- Se puede crear belleza con un computador
- Los computadores puden cambiar la vida para mejor

HACKTIVISMO

- **Activismo que se ayuda de las TIC para hacer llegar su mensaje. Podrían llegar a hacer, ayudar, motivar ataques contra los sistemas informáticos, por lo general páginas web o servidores de correo electrónico de las instituciones o grupos seleccionados.**
  - Un grupo con una causa sobrecarga servidores de correo electrónico y hackea los sitios Web con mensajes para sus causas.
  - Los ataques no tienen intención de ser perjudiciales, aunque podrían causar daños en los servicios

- **¿Conoceis/Recordais algún ataque?**

HACKER

Según los gobiernos y la prensa, también serían hackers los que se aprovechan de las debilidades de los sistemas informáticos para:

- Terrorismo
- Extorsión
- Espionaje político y militar
- Espionaje empresarial
- Odio, bulling …
- Para ganar fama

Según la definición, ¿todos estos serían crakers?

HACKER

Según los gobiernos y la prensa, también serían hackers los que se aprovechan de las debilidades de los sistemas informáticos para:

- Conseguir los correos de un político importante y hacerlos públicos
- Conseguir los correos internos de una entidad empresarial y hacerlos públicos
- Conseguir la lista de clientes de una web de citas y hacerlos públicos
- Conseguir un video privado de un particular y hacerlo público
- Conseguir entrar a metanet (no modificar nada) pero explicar públicamente cómo se hace
- Para la infraestructura informática de una dictadura por orden de un gobierno democrático

Según la definición, ¿todos estos serían crakers? ¿Sería ético?

OPINIÓN, REFLEXIÓN

¿PUEDEN AYUDAR A HACER EL MUNDO MEJOR?

HACKERS

No todos los profesionales de las TICs consideran a los hacker (aún siguiendo su definición) como buenos para el sistema

- **Supone un sobre-coste aunque los ataques no causen daño**
  - Poneman Institute [13] , estima que el coste por violación de datos fue de 2,7 millones de dolares en 2010 sólo en EEUU (214$ por usuario)
- **Tiene consecuencias sociales**
  - Podría tener efectos psicológicos en las personas “atacadas”
  - Tiene claramente efectos de perdida de privacidad auspiciado por las empresas para intentar disminuir estos “ataques”