

DIRITTO
ANNO 2020-21

DIRITTO **DELL'INFORMATICA**

Simone Biondo



INTRODUZIONE	5
Che cos'è il diritto dell'informatica?	5
Diritto pubblico e diritto privato	6
Dov'è il diritto e da dove lo si conosce?	6
Regolare l'informatica	7
SANZIONI	8
Le sanzioni amministrative e penali	8
NET NEUTRALITY	9
Principio di neutralità della rete	9
Costi per l'accesso alla rete e dichiarazione dei diritti di Internet	9
Net neutrality: solo un'aspirazione politica?	10
SOCIETÀ DELL'INFORMAZIONE	11
Verso una nuova società	11
Identità digitale	11
Il concetto di dato	11
Il documento informatico	12
Posta elettronica certificata: PEC	12
Blockchain	13
Smart contract	13
Riassunto e approfondimenti	14
TRATTAMENTO DEI DATI PERSONALI	15
Dati personali e riservatezza	15
Il diritto alla riservatezza e l'Unione Europea	16
Diritto all'oblio	17
Riassunto e approfondimenti	17
LA PROTEZIONE DELLA PRIVACY	18
Privacy e libertà personali	18
Registro delle opposizioni	18
Social network e privacy	19
Il contratto nei social network	20
Riassunto e approfondimenti	21
IL COMMERCIO ELETTRONICO	22
La vendita a distanza	22

Ostacoli al commercio elettronico	23
Riassunto e approfondimenti	25
I CONTRATTI A DISTANZA	26
Il codice del consumo: linguaggio chiaro e comprensibile	26
Il diritto di recesso	27
Un esempio di servizio a distanza: il cloud computing	27
Le aste online	28
Riassunto e approfondimenti	28
GLI SMART CONTRACT	29
Smart contract come contratti vincolanti	29
IL DIRITTO D'AUTORE	30
Il diritto d'autore: storia	30
Il diritto d'autore come forma di salvaguardia	31
Il diritto d'autore nell'informatica	32
Le banche dati	32
Come proteggere gli autori?	33
Riassunto e approfondimenti	34
LE MONETE E I MEZZI DI SCAMBIO VIRTUALI	35
Le prime forme di scambio	35
Carte di credito e carte di debito	35
La moneta elettronica	36
Le criptovalute	36
La moneta virtuale secondo l'Unione Europea	37
Unità di conto virtuale	37
Riassunto e approfondimenti	38
REATI INFORMATICI	39
Che cosa si intende per reato?	39
I reati informatici	40
IL CODICE DELL'INFORMATICA	43
Le regole nell'informatica: la mancanza di un codice specifico	43
Il codice delle telecomunicazioni	44
Il diritto dell'informatica nel mondo	45
NOMI DI DOMINIO	46
Il marchio	46
Il nome di dominio	47

DOMANDE FINALI	48
DOMANDE RAPIDE FINALI	53

INTRODUZIONE

Che cos'è il diritto dell'informatica?

Viene così chiamato perché comprende tutte le regole che parlano dell'informatica. È una disciplina che cerca di trovare ordine per le regole che si sono accatastate negli anni. Queste regole non hanno una spina dorsale, non abbiamo dei fondamenti che ci consentono di dare principi fissi in tutte le situazioni. Poiché le regole sono molte, se c'è ordine ci si riesce ad orientare, altrimenti ci si perde. Quando parliamo di diritto dell'informatica, il filo conduttore è la tecnologia. Il corpo di regole importante per trattare questioni tecnologiche viene chiamato il **codice dell'amministrazione digitale**. Tuttavia, la sua funzione non è regolare i rapporti tra privati ma disciplinare i rapporti della pubblica amministrazione. Prima di procedere bisogna capire cos'è il diritto. Se l'informatica è una scienza esatta, lo stesso non si può dire del diritto. Il diritto è una scienza umana, cioè una scienza del linguaggio che **si esprime con parole**. Questo spiega il problema del senso del linguaggio privo di oggettività. Il linguaggio dipende dal contesto e dai sensi che si possono attribuire alle parole. Poiché non c'è la prova scientifica della verità delle parole, abbiamo la necessità di ridurre la **zona grigia**, ovvero la situazione di incertezza delle regole. Le leggi vanno quindi **interpretate** in relazione al contesto e non applicate e basta. Il diritto è un insieme di ordini. Le regole non raccontano una storia, ma un comando, il diritto è posto da un'autorità che può fare le regole. Queste regole sono obbligatorie e l'ordinamento reagisce. Il diritto è fatto di regole formali che possono essere consultate. Le leggi restano in vigore finché non vengono abrogate. Le leggi in Italia sono abrogate anche per **incompatibilità**: se due leggi sono incompatibili, la legge precedente viene abrogata. La compatibilità, essendo un giudizio riprende il problema del linguaggio. Per questo motivo di incomprensione nemmeno il legislatore sa quali norme sono ancora vigenti.

Diritto pubblico e diritto privato

Si sente spesso parlare di varie tipologie di diritto: diritto civile, diritto penale e, per esempio, diritto amministrativo. In realtà sono due le grandi partizioni fondamentali del diritto: il **diritto pubblico** e il **diritto privato**. Nel diritto pubblico, abbiamo sempre un'**autorità che può esercitare potere** perché la legge glielo consente (potere dato dalla Costituzione). Il diritto privato invece, è l'insieme delle regole in cui due soggetti possono contrattare i loro rapporti, non sono obbligati da alcuna autorità ed è quindi il diritto dove **nessuno comanda**. Nel diritto dell'informatica si tratta di gran parte di diritto privato (anche se non tutto, per esempio, il codice dell'amministrazione digitale dice alle pubbliche amministrazioni che cosa devono fare). Ciò ci dà tutela perché possiamo rivolgerci a esse.

Dov'è il diritto e da dove lo si conosce?

Il documento che ci dice qual è il diritto è la **Gazzetta Ufficiale**, il luogo dove si trovano tutte le leggi. Finché una legge non si trova sulla Gazzetta Ufficiale non è valida. Per quanto riguarda la **legge**, essa si riferisce a un **provvedimento emanato dal Parlamento**, Camera e Senato. Il governo, che ha la fiducia del Parlamento è quell'organo che ha il compito di amministrare l'Italia. Il Parlamento fa le leggi e il governo amministra. Poiché noi votiamo il Parlamento e non il governo, la Costituzione è stata ben attenta a dire che il governo non può fare le leggi. Tuttavia ci sono le emergenze. Se ci aspettassimo che il Parlamento facesse una legge per regolare le emergenze, poco o nulla si risolverebbe. Il governo in casi straordinari e di necessità e urgenza, può fare **decreti legge**. Per rispettare il principio democratico, per cui le leggi le fanno i soggetti che risiedono in Parlamento, questi decreti legge devono essere convertiti per essere trasformati in legge effettiva. Questa conversione deve essere effettuata entro 60 giorni, altrimenti il decreto sparisce, ovvero decade.

Regolare l'informatica

L'Italia non è al di fuori dei rapporti con tutti gli altri paesi. Delle volte possono nascere delle convenzioni, importanti in materia informatica, poiché essa non ha confini. Queste convenzioni non sono altro che accordi tra paesi per regolamentare diverse questioni e ce ne sono molte in ambito informatico. L'Italia prima di tutto fa parte dell'Unione europea, la quale fa effettivamente regole. Le regole dell'Unione europea sono di diverso tipo, le principali sono i **regolamenti** e le **direttive**. Un regolamento è un atto legislativo vincolante che deve essere applicato in tutti i suoi elementi nell'intera Unione europea, mentre una direttiva è un atto legislativo che stabilisce un obiettivo che tutti i paesi dell'UE devono realizzare (tuttavia, spetta ai singoli paesi definire attraverso disposizioni nazionali come tali obiettivi vadano raggiunti). In materia di diritto dell'informatica, il diritto di derivazione dell'Unione europea è massiccio e prepotente in senso positivo.

SANZIONI

Le sanzioni amministrative e penali

In ambito informatico sentiremo spesso parlare di sanzioni. Nel linguaggio di tutti i giorni siamo abituati a parlare di multe: poiché i termini hanno un loro significato, bisogna prestare attenzione. Nel nostro ordinamento, le sanzioni sono di due tipi: **sanzioni di tipo amministrativo** e **sanzioni di tipo penale**. Nel passato, con la violazione di una norma, la sanzione era solo di tipo penale o tendenzialmente penale. Nel dopoguerra la violazione di alcune norme con conseguente sanzione penale, parve troppo grave: questo perché le sanzioni che appartengono al diritto penale hanno un **afflittività molto elevata**, devono essere inflitte da un giudice e comportano spesso delle conseguenze gravissime. Il codice penale prevede delle sanzioni che sono indicate in modo **testuale**, cioè non c'è possibilità di sbagliarsi. Si parla di arresto o reclusione per i delitti o le contravvenzioni. Si parla di multa o ammenda per le sanzioni di tipo economico. I delitti sono reati più gravi, mentre le contravvenzioni sono reati meno gravi, i delitti sono dolosi, mentre le contravvenzioni sono sia dolose e colpose. L'aspetto essenziale dei reati regolati dal codice penale è che devono essere **inflitte necessariamente da un giudice**. Questo aspetto molto macchinoso, dove è richiesta la presenza di un giudice è sproporzionato per quei comportamenti illegittimi di piccola rilevanza. Le sanzioni che riguardano questi comportamenti vengono pertanto inflitte da un'autorità amministrativa. Quindi le **sanzioni che non riguardano la libertà delle persone** possono essere inflitte dalla **pubblica amministrazione** attraverso i propri funzionari.

NET NEUTRALITY

Principio di neutralità della rete

Tra i principi fondamentali in materia di informatica troviamo il **principio di neutralità della rete**. Questo principio attiene alla regola di non discriminazione degli utenti, del diritto a tutti gli utenti di entrare in rete con dati che vengono immessi e con dati che vengono scaricati. Questo principio nasce come richiesta, pretesa di alcuni movimenti che affermavano che non è possibile discriminare l'accesso alla rete. Come per il diritto alla libera circolazione, anche nella rete vogliamo muoverci liberamente, senza pregiudizi. Questa è sicuramente la conquista della modernità.

Costi per l'accesso alla rete e dichiarazione dei diritti di Internet

L'accesso alla rete ha dei **costi**. I provider che gestiscono la rete hanno sicuramente vari costi di aggiornamento, manutenzione, controllo e protezione, tanto per citarne alcuni. Questi costi in realtà sono enormi: il principio di non discriminazione deve anche tenere conto delle ragioni economiche (come dice la prima legge dell'economia, la minestra non è gratis per nessuno, nessuno può mangiare senza pagare). Ciò significa che i costi per la rete vanno in qualche modo supportati. Per esempio, chi immette o scarica più dati dalla rete deve necessariamente pagare di più. Ma cosa dice di preciso il principio di neutralità della rete? Nel documento '**dichiarazione dei diritti di Internet**', nell'articolo 4 si dice così: *ogni persona ha il diritto che i dati trasmessi e ricevuti in Internet non subiscano discriminazioni, restrizioni, interferenze in relazione al mittente e ricevente, tipo e contenuto dei dati, dispositivo utilizzato, applicazioni o in generale legittime scelte delle persone. Il diritto a un accesso neutrale di Internet nella sua interezza è necessario per i diritti fondamentali della persona.* Il valore normativo di tale dichiarazione è **pari a zero**. Questo documento non vale niente. Questo perché la dichiarazione è stata fatta da un soggetto a cui nessuna norma ha attribuito il potere di creare regole.

Net neutrality: solo un'aspirazione politica?

Nel tempo c'è stata un'altra deliberazione fatta dall'**autorità delle telecomunicazioni**. Anche in questo caso, nonostante si affermino vari principi come quello della net neutrality, tale documento non ha alcun valore normativo. Si tratta di una delibera che non vincola nessuno a fare niente: insomma, tante belle parole, ma nessun diritto, cioè nessun testo normativo vincolante che obblighi Internet a comportarsi nel modo richiesto. Esiste un principio giuridico della net neutrality o è solo un'**aspirazione politica**? In Italia abbiamo il **codice delle telecomunicazioni** che regola diverse questioni. L'articolo 4 di tale codice enuncia una serie di diritti. L'articolo 2 dice che a garanzia di diritti quali libertà di comunicazione, segretezza di comunicazione e libertà di iniziativa economica, gli obblighi per le imprese che forniscono reti e servizi di comunicazione elettronica sono imposti secondo principi di trasparenza, non distorsione della concorrenza, **non discriminazione** e proporzionalità. Inoltre l'articolo 13 dice che il ministero e l'autorità delle telecomunicazioni, perseguono, ove possibile, il **principio di neutralità tecnologica**. Con questo principio di neutralità tecnologica si è fatto un passo avanti: dalle aspirazioni politiche, siamo passati a regole che impongono la neutralità. Ma questa non discriminazione è rivolta alle imprese quindi non siamo ancora arrivati alla net neutrality per l'utente finale, ovvero i cittadini. Nel 2015 l'Unione europea ha emanato un **regolamento** in tale materia. Le misure di questo regolamento rispettano il principio di neutralità della rete, vale a dire non impongono, ne favoriscono l'utilizzo di un determinato tipo di tecnologia. In particolare: *gli utenti dovrebbero avere il diritto di accedere a informazioni e contenuti e di diffonderli, nonché usufruire di servizi senza discriminazione. Inoltre, i fornitori di tali servizi dovrebbero trattare tutto il traffico allo stesso modo, senza discriminazioni, restrizioni o differenze, a prescindere dalla fonte o dalla destinazione dei contenuti*. Poiché queste sono le volontà del legislatore dell'Unione europea, tutti questi punti sono espressi nel regolamento vero e proprio. Siamo così passati dal codice delle telecomunicazioni che si riferisce alle sole imprese o al ministero e autorità agli utenti finali, indicati nel regolamento stesso. In seguito a tale regolamento, l'autorità delle telecomunicazioni ha espresso che i fornitori di accesso a Internet devono consentire che il cliente possa scegliere le proprie apparecchiature terminali e non possa imporre loro la fornitura in modalità esclusiva.

SOCIETÀ DELL'INFORMAZIONE

Verso una nuova società

Parliamo spesso di **società dell'informazione**. La libertà di informazione, la libertà di impresa consentono a chiunque di trasmettere. In particolare, con l'avvento della tecnologia si è imposta la **virtualità alla fisicità**, nella creazione, trasmissione e conservazione senza confini, né di tempo né di luogo. Ciò ha creato la società e l'economia dell'informazione con nuovi modi di creare ricchezza, nuovi modi di comunicare ma anche nuovi pericoli. In questo nuovo mondo esiste il tema dell'**analfabetismo digitale** (incapacità delle persone di operare mediante un computer, di leggere, scrivere e reperire criticamente informazioni in Internet), comprendente ampie fasce della popolazione, soprattutto negli anziani. Un'altro punto cardine della società dell'informazione è l'esistenza dei social network. La nascita di questa nuova società è un fenomeno imponente che non può essere trascurato, soprattutto per l'**accumulo dei dati personali** che vengono quotidianamente immessi e che si interfacciano con i **problemi della tutela della persona**. Qualsiasi opinione espressa è un dato a disposizione di altri.

Identità digitale

Il problema dell'**identità digitale**, cioè l'insieme dei dati che riguardano un certo soggetto è enorme. Possiamo parlare dell'identità digitale come concetto giuridico legato al concetto di identità. Legato al concetto dell'identità digitale, c'è il **diritto all'oblio**, cioè la necessità di essere dimenticati. In ambito di dati si può avere il bisogno di eliminare informazioni sul proprio conto.

Il concetto di dato

Fino ad ora abbiamo parlato di dato, ma che cos'è il dato? Nell'ambito del diritto un dato è un'insieme di informazioni. Chi raccoglie dati su di noi è poi in grado di venderli. I dati sono quindi un bene spendibile sul mercato. Quando entriamo in rete paghiamo con la nostra **profilazione**. Nell'economia digitale abbiamo quindi una moneta nuova che non è più il denaro ma il dato.

Il documento informatico

Un altro concetto di cui parlare è quello di documento informatico: non si parla più di carta scritta con il termine documento. Che valore ha un file nella modernità, quando l'abitudine spinge a pensare al documento come foglio scritto e firmato? Il codice dell'amministrazione digitale ha risposto a questa domanda, dando un valore concreto al file con delle sottigliezze. Un file può essere scritto e modificato molte volte. Come facciamo a riconoscere l'autore di una particolare versione? In base a cosa si deduce l'appartenenza di un file e qual è la sua firma? Si pone il problema della **riferibilità del file**. La firma di questi documenti si avvale di strumenti informatici. La **firma digitale**, per esempio, viene allegata al documento e nel momento in cui un file viene modificato, anche la firma stessa viene cambiata. La prima cosa che si fa per controllare la validità di un documento è solitamente la verifica delle firme. Per poter apporre la firma digitale è necessaria l'esistenza di un soggetto esterno, il **certificatore**, che, tra i suoi vari poteri identifica con certezza, il titolare del certificato qualificato, i suoi poteri, ed i suoi limiti. Le firme hanno una **validità temporale**. Il rinnovo del proprio certificato digitale può essere effettuato dal titolare nei 90 giorni che precedono la data di scadenza.

Posta elettronica certificata: PEC

Tipico elemento della società dell'informazione è la posta elettronica. La mail è un **documento digitale trasmissibile**: come per la firma digitale, anche la mail deve avere un meccanismo di riconoscimento. Con la posta elettronica certificata, una comunicazione fa uso di un riconoscimento per identificare a chi appartiene l'indirizzo email.

Blockchain

Un'altro aspetto chiave della società dell'informazione è l'utilizzo della tecnologia blockchain. È definita come un **registro digitale** le cui voci sono raggruppate in blocchi, concatenati in ordine cronologico, e la cui integrità è garantita dall'uso della crittografia. Sebbene la sua dimensione sia destinata a crescere nel tempo, è **immutabile** in quanto, di norma, il suo contenuto una volta scritto non è più né modificabile né eliminabile, a meno di non invalidare l'intera struttura. Ad un blocco possono essere associate una o più **transazioni** e ogni blocco, inoltre, contiene un puntatore hash al blocco precedente e una **marca temporale**. La tecnologia blockchain impedisce agli utenti malevoli di interferire con le operazioni di transazione delle criptovalute. Questa tecnologia, che è in pieno sviluppo e sta affrontando diverse innovazioni, viene valutata dalle banche centrali per vedere se le amministrazioni pubbliche possono utilizzarla in modo proficuo in quanto richiede un'**elevata potenza di calcolo** per poter interferire con le **operazioni sensibili** nella rete.

Smart contract

Un altro tema caro ai giuristi è quello degli **smart contract**: sono protocolli informatici che facilitano, verificano o fanno rispettare la negoziazione o l'esecuzione di un contratto. Tuttavia, ci sono situazioni per cui è difficile realizzare smart contract, soprattutto se le **variabili** da valutare sono molte e dipendono dal contesto e possono influire sulla correttezza dell'adempimento: **regolare un contratto in maniera algoritmica** diventa complesso. Inoltre il codice civile quando affronta il **problema dell'adempimento** affronta anche il **problema dell'impossibilità**. Com'è che si determina con i dati che possono essere ricevuti da un algoritmo questa impossibilità o disinteresse nell'adempimento? Questo chiaramente è un problema e i margini di funzionamento in alcuni contesti sono ridotti.

Riassunto e approfondimenti

Servizi delle società dell'informazione: servizi prestati solitamente (quindi non sempre) dietro retribuzione, per via elettronica e a richiesta di un destinatario di servizi che non è per forza un consumatore ma è il soggetto che usa i servizi. Esempio: vendita online di merci.

Il concetto di riferibilità: un file contiene un valido documento quando l'autore è identificabile (firma digitale), i dati sono immutabili, il documento è integro e non contiene codice che modifica il contenuto del documento stesso.

PEC: la PEC è obbligatoria per pubbliche amministrazioni, imprese, professionisti iscritti in albi ed elenchi istituiti con legge.

Firma elettronica avanzata: insieme di dati allegati/connessi ad un documento che garantiscono la connessione univoca al firmatario e permettono di rilevare se i dati sono poi stati modificati. Un esempio è la firma digitale che deve essere basata su un certificato qualificato e su crittografia asimmetrica: criptato con chiave pubblica e decriptato con chiave privata.

Fascicolo telematico: versione informatica del fascicolo d'ufficio, contenente gli atti del processo come documenti informatici oppure le copie informatiche dei medesimi atti.

Wireless community network: insieme di persone che crea una rete di comunicazioni wireless, cittadini che mettono access point, fuori dalle loro case, collegati tra loro. **Non c'è amministrazione gerarchica**: ogni utente può cambiare IP quando vuole quindi rimane anonimo, inoltre la WCN non è sottoposta ad alcuna autorità in quanto dipende dai soli accordi degli aderenti.

TRATTAMENTO DEI DATI PERSONALI

Dati personali e riservatezza

Parliamo ora di un tema che svolge un ruolo importante nelle relazioni sociali, il **trattamento dei dati personali** e il **diritto alla riservatezza**. Questo tema, esploso a partire da metà degli anni 90 ha radici lontane. Di seguito si elencano dei passaggi importanti.

Caso Caruso: a metà degli anni '50 la Cassazione segnalò un buco nel sistema del diritto, in particolare riguardante il capitolo del diritto alla riservatezza. La questione era sorta in merito al caso del celebre tenore Enrico Caruso. Senza entrare nello specifico, il caso riguardava la divulgazione di dati strettamente personali del tenore tramite due pellicole cinematografiche.

Caso Petacci: A metà degli anni '60, grazie a questo caso ci fu un avvicinamento concreto della Corte suprema verso il diritto alla privacy. Il caso riguardava la pubblicazione di un libro su l'amante di Mussolini (Clara Petacci) dove, secondo i familiari della Petacci, vi erano scritte informazioni troppo personali che potevano ledere la sua figura pubblica, minandone la reputazione.

Caso Esfandiari: Nel 1975 il Supremo Collegio formula, tramite la consultazione di una copiosa giurisprudenza in merito, la mutazione dell'ordinamento giuridico di fronte alla tutela dei dati sensibili personali. La sentenza infatti affermava costituire lesione della privacy la divulgazione di immagini o avvenimenti non direttamente rilevanti per l'opinione pubblica. La pronuncia veniva resa in particolare nel caso di Soraya Esfandiari Bakhtiari, dove alcuni giornali avevano pubblicato fotografie ritraenti l'ex imperatrice (di Persia) in atteggiamenti intimi con un uomo nelle mura della propria abitazione.

Il diritto alla riservatezza e l'Unione Europea

Il diritto alla riservatezza ormai è diventato fondamentale con l'avvento della tecnologia: l'Unione europea ha deciso di dare vita a regole per la protezione dei dati personali. Il **regolamento 679 del 2016 dell'Unione europea** ha imposto ai vari Stati la necessità di rivedere il diritto alla privacy. Il regolamento ha come perno di funzionamento, il consenso che ognuno deve dare affinché i dati personali vengano in qualche modo trattati. Il **consenso deve quindi essere espresso in modo chiaro** (il silenzio assenso non riguarda i privati e non è un'opzione valida). Ci sono casi di esenzione, cioè in alcuni contesti, i dati personali possono essere trattati senza consenso, per esempio per ragioni di giustizia. Il consenso è **revocabile**, non è una scelta definitiva, non esistono impegni eterni. Il consenso va poi rapportato con la nozione di dato, cioè qualsiasi informazione che ci riguarda. Questa informazione può essere di vario tipo: **dati sensibili** come le idee politiche e gli orientamenti religiosi e i **dati ultrasensibili** che riguardano la sfera sessuale e i dati clinici. Questi dati **devono essere raccolti con certe modalità**. Innanzitutto abbiamo il **principio generale dell'anonimato**, cioè i dati personali devono essere raccolti solo quando si rendono necessari per raggiungere un determinato scopo, altrimenti devono essere raccolti in modo anonimo. I dati vanno poi **raccolti in modo corretto**, cioè devono essere coerenti con la realtà. Devono poi essere raccolti secondo il **principio di minimizzazione**, cioè vengono raccolti solo quei dati che servono per una determinata funzione e non dati personali irrilevanti. Da parte della persona esiste il diritto al rispetto di tali regole: ognuno di noi ha il diritto di sapere chi conserva i propri dati personali e quali dati hanno a disposizione. Questo diritto è protetto da sanzioni enormi per chi non lo rispetta. I dati devono poi essere **conservati solo per il tempo necessario** per cui vengono raccolti. Ci sono poi **misure di sicurezza** per evitare che i dati personali vengano sottratti: in casi di furto delle informazioni è chi li conserva che ne deve rispondere. Ogni volta che riteniamo ci sia una violazione dei nostri diritti, possiamo rivolgerci o al giudice o all'autorità garante per la tutela dei dati personali. In generale, però, **la profilazione è il prezzo che paghiamo per usufruire dei servizi della rete**.

Diritto all'oblio

Capiamo quindi l'esigenza del diritto all'oblio, cioè il **diritto di essere dimenticati**. Tale diritto è motivato da regole espresse. Tuttavia, se siamo nell'ambito degli eventi storici, nessuno può pretendere la cancellazione di un dato: la storia appartiene alla collettività. Se un evento non appartiene alla storia ma appartiene alla cronaca, cioè l'attualità, non può essere diffuso senza il consenso.

Riassunto e approfondimenti

Trattamento dei dati personali: operazioni su dati contenuti in banche dati e non.

Principio di necessità nel trattamento dei dati personali: identificare l'interessato solo se serve. Bisogna solo raccogliere i dati necessari e non altri.

Dato personale: permette l'identificazione di una persona.

Dato sensibile: rivela l'origine razziale/etnica, convinzioni, dati di salute e vita sessuale.

Cookies: avvisare l'uso di cookies serve per tutelare la privacy degli utenti che possono scegliere di non usare i cookies (tecnici e di profilazione).

LA PROTEZIONE DELLA PRIVACY

Privacy e libertà personali

La protezione della privacy è un problema che riguarda la nostra libertà, c'è un'intersezione tra la tecnologia che consente di invadere la privacy e conservare i dati personali con il diritto di non trovarsi in situazioni di questo tipo.

Registro delle opposizioni

Uno degli esempi a cui siamo abituati, cioè situazioni in cui subiamo spesso un'invasione della nostra sfera personale è quello delle **spam**. Offerte commerciali e proposte di tipo economico invadono la nostra posta elettronica al punto tale che esistono fornitori di posta elettronica che dividono queste offerte dalle comunicazioni. La legge in teoria prevede un rimedio a questa invasione di comunicazione di tipo commerciale. È stato infatti creato il **registro delle opposizioni**, dove possiamo chiedere di non ricevere comunicazioni di tipo commerciale. Per fare ciò è necessario iscriversi a tale registro.

Social network e privacy

Un'altro aspetto che attiene ai nostri rapporti con qualcuno che invade la nostra sfera personale, per esempio con la comunicazione e la profilazione attraverso dati personali è quello dei **social network**. Che implicazioni ha la nostra relazione con i social network? In questo momento c'è un'**assenza grave di regole** che riguardano tali servizi. Ciò pone una serie di problemi: i giuristi sono costretti a utilizzare regole di carattere generale che devono essere **adattate** con la perdita di una tutela adeguata. Le autorità (quelle che non possono porre regole) spingono per l'**autoeducazione**. Ciò ovviamente non funziona in quanto i rischi sono molti e non c'è voglia e tempo di prestare attenzione, oltre che la presenza di una certa riluttanza. Quindi, quando una persona immette dati in un social network, questi sono irremovibili. Tra tutte sono necessarie regole per aggressioni psicologiche realizzate tramite strumenti informatici. Sono ormai tristi e famosi i casi di cyberbullismo che negli ultimi anni hanno colpito diversi adolescenti e non solo. Servono quindi regole specifiche che hanno come punto di partenza l'utilizzo della tecnologia. Dal profilo tecnologico i social network non sono altro che un servizio offerto da un internet provider: un internet provider che svolge solo **attività di hosting**, cioè che permette alle persone di caricare file, messaggiare, comunicare, in generale **non è responsabile di ciò che viene pubblicato**, a meno che non abbia collaborato con colui che abbia caricato le informazioni o si rifiuti di rimuovere un'immagine offensiva. Nel momento in cui un social network ci mette a disposizione questo servizio, accettando di utilizzarlo secondo le condizioni proposte, stiamo stipulando un vero e proprio **contratto a titolo gratuito**, anche se in realtà gratuito non è, a causa di **profilazione e trasferimento di dati personali a terzi**. Nel 2019 sono state emanate direttive (per cui gli Stati membri devono emanare le legislazioni interne necessarie per l'applicazione di esse), dove viene indicato l'obbligo di comunicare all'utente che il contratto non viene pagato con denaro ma con la **cessione dei dati personali**. Entrare in un social network significa quindi concludere un contratto e ogni contratto ha delle regole specifiche.

Il contratto nei social network

I contratti regolati dal codice civile vengono chiamati i **contratti tipici**. Il codice civile ha inoltre consentito alle persone di inventarsi dei contratti, i cosiddetti **contratti atipici**. Il rapporto con un internet provider è un contratto atipico, non abbiamo regole che lo disciplinano. Ma ciò non vuol dire che non vengono presi in considerazione dal legislatore. Il codice civile, però, specifica al suo interno alcune **regole inderogabili per tutti i tipi di contratto** che si devono obbligatoriamente rispettare. Questi obblighi sono anche chiamati **norme imperative** (nel diritto pubblico ci sono solo norme imperative). Le norme, invece, che possono essere cambiate si chiamano **norme dispositive**, consentendo quindi più libertà. Una norma imperativa nell'uso dei social network è quella che dice che *sono nulle le clausole che limitano la propria responsabilità nei casi di dolo o colpa grave*. Cominciamo a dire che il rapporto che abbiamo con un internet provider che eroga servizi di social network è **regolato dalle clausole accettate prima di entrare**. Quali sono quindi le regole dei social network? Ci sono innanzitutto le **condizioni di contratto**. Ci sono poi sezioni come la **policy che riguarda la privacy** e in che modo protegge gli utenti: questo è uno degli obblighi che nascono dal regolamento 679 del 2016. Poi ci sono le regole definite come **etiche della Community**: anche se sembrano regole di buona educazione, in realtà sono condizioni generali di contratto e non hanno quindi solo un valore di rapporto sociale, ma un valore che è propriamente giuridico. Chiunque entri in un social network può in un secondo momento uscire, quindi può **recedere dal contratto**. Nel caso di recessione, il problema risiede nei dati personali immessi. La tutela dell'utente in relazione ai dati che immette in un social network è quella data dal regolamento sulla privacy. Questa autorizza l'utente a pretendere la cancellazione di tutti i suoi dati e ottenere la conferma da colui che li ha, dell'effettiva eliminazione. Tuttavia, di fronte alla dichiarazione dell'Internet provider di aver cancellato i dati, l'unica tutela dell'utente è la **fiducia**.

Riassunto e approfondimenti

Web reputation: raccolta/monitoraggio di dati presenti nel web riguardanti un certo prodotto/servizio/evento.

Privacy seals: marchi di organizzazioni indipendenti che dicono che un certo sito rispetta le privacy policies.

Codici di condotta: secondo il GDPR dal 2016, sono strumenti di autodisciplina adottati su base volontaria attraverso i quali i rappresentanti e associazioni di categoria possono far prevalere regole interne di protezione dei dati personali.

IL COMMERCIO ELETTRONICO

La vendita a distanza

Il commercio elettronico rappresenta una delle anime in cui l'informatica ha conquistato il mondo. Prima che ci fosse Internet, come funzionava la vendita a distanza? La vendita a distanza si chiama così perché non c'è uno dei due soggetti che si reca dall'altro, **non c'è un incontro fisico**. In origine c'era il sistema dei cataloghi: si riceveva a casa il catalogo della merce, si sceglieva una cartolina da inviare al venditore per ricevere ciò che si aveva deciso di comprare. Con l'avvento delle TV private nasce la **pubblicità** il cui unico mezzo fisico è la televisione. Con la pubblicità e l'utilizzo curato di immagini, si è visto aumentare notevolmente l'efficacia della vendita a distanza, tant'è che a partire da ciò ci sono stati diversi interventi del legislatore dell'Unione europea che ha cominciato a porre delle regole per proteggere i consumatori. Si sono rese necessarie regole specifiche per controllare il fenomeno delle pubblicità a **tutela del consumatore**. Dalle televisioni si è poi passati al computer: questa transazione ha cambiato il consumatore che **da soggetto passivo è diventato soggetto attivo**, cioè un consumatore in grado di effettuare operazioni di compravendita a distanza, in maniera interattiva e in totale autonomia. Sono quindi servite nuove regole perché quelle che tutelavano il consumatore, inteso come un soggetto passivo, non si sono rese valide in questo nuovo contesto.

Ostacoli al commercio elettronico

Con la direttiva 31 del 2000 l'Unione europea ha cercato di regolare alcuni aspetti giuridici dei servizi della società dell'informazione, in particolare il commercio elettronico nel mercato interno dell'Unione europea. Con questa direttiva si è cercato di eliminare i diversi ostacoli di tipo giuridico al commercio elettronico: per esempio è richiesta la **necessità che non ci siano autorizzazioni a chi voglia svolgere la propria attività utilizzando la rete**. Tra i considerando della direttiva, in particolare il numero 10, troviamo quanto segue: *le misure previste dalla presente direttiva si limitano al minimo necessario per raggiungere l'obiettivo del buon funzionamento del mercato interno*. Questo vuol dire che i vari ordinamenti dei singoli Stati possono ampliare, non ridurre, il contenuto della direttiva per favorire la rimozione degli ostacoli. Qual è il primo problema che si pone? Il primo problema è che **non deve esserci un'autorizzazione di tipo discrezionale**. Gli ordinamenti non devono poter scegliere chi può svolgere servizi e chi non. Questo poiché dal profilo dell'informazione corrisponderebbe a una censura quanto al profilo dell'attività commerciale sarebbe una selezione tra soggetti che operano e quelli che non vengono autorizzati. Se ciò si verificasse, ci sarebbe una **restrizione della concorrenza che è totalmente contrario ai principi dell'Unione europea**. In questa direttiva troviamo soprattutto regole di libertà: questa direttiva ha abbracciato tutti gli utenti, dagli utenti privati, cioè ognuno di noi, ma anche quelli che utilizzano Internet per motivi di lavoro. Questa sottolineatura è importante perché vedremo che il codice del consumo protegge solo il consumatore. Tra i vari considerando, troviamo anche l'obbligo degli Stati membri di **togliere ogni ostacolo nei contratti elettronici**, ovvero tutti quei contratti che facciamo nel momento in cui effettuiamo transazioni online. Per esempio il punto 2 dell'articolo 3 dichiara che *gli Stati membri non possono limitare la libera circolazione dei servizi tipici della società dell'informazione provenienti da un'altro Stato membro*. Un'altro aspetto importante è il principio di **assenza di autorizzazione preventiva**: gli Stati membri garantiscono che l'attività del prestatore non sia soggetta ad autorizzazione preventiva. La direttiva si occupa in generale di 2 questioni: da una parte le informazioni che si danno obbligatoriamente a chi accede ai servizi, dall'altra gli obblighi di controllo e di verifica a carico di chi svolge attività di Internet provider, in particolare l'attività di hosting. In merito all'attività di hosting nella direttiva si dichiara che *gli Stati membri non impongono ai prestatori un obbligo generale di sorveglianza sulle informazioni che trasmettono e memorizzano, né un obbligo di ricercare attivamente fatti o circostanze che indicano la presenza di attività illecite*.

Se ciò non fosse stato dichiarato nella direttiva si sarebbe assistito alla chiusura delle attività di hosting. Riprendendo invece le regole sui comportamenti obbligatori in merito al commercio elettronico, si sono voluti **garantire all'utente una serie di informazioni e dati per avere protezione quando il servizio non va buon fine** (come ritardi di consegna, prodotto non conforme e altri esempi). Il cliente deve essere sempre in grado di trovare la controparte con cui lamentarsi. Nell'articolo 5 troviamo una serie di dati, ovvero una serie di informazioni generali da fornire all'utente: per esempio il nome del prestatore, il suo indirizzo geografico, oltre ad altre informazioni, come l'indirizzo di posta elettronica. Tutte queste informazioni devono essere recapitate in un **formato stabile e duraturo**, cioè si possono conservare. Un'altro aspetto importante sono le informazioni commerciali. La comunicazione commerciale deve essere chiaramente identificabile come tale, ciò significa che l'utente deve essere consapevole di star ricevendo una proposta di tipo commerciale. Inoltre viene richiesto agli Stati membri di adottare provvedimenti per far sì che i prestatori dei servizi che desiderino effettuare comunicazioni commerciali consultino regolarmente i **registri negativi** in cui possono iscriversi le persone fisiche (cioè il registro delle opposizioni in Italia). Altro importante aspetto della direttiva è l'articolo 11: *il prestatore deve informare l'avvenuta ricevuta dell'ordine e gli Stati membri devono assicurarsi che il prestatore metta a disposizione del destinatario del servizio strumenti tecnici adeguati per correggere eventuali errori di inserimento dei dati*. Infine la direttiva mette a disposizione **articoli per gestire le controversie** nel commercio elettronico.

Riassunto e approfondimenti

Marchi di qualità: servono ad accrescere la fiducia degli acquirenti nei confronti del commercio elettronico, attestando che il fornitore online certificato si attiene a determinati standard/principi e criteri nel condurre operazioni commerciali.

I CONTRATTI A DISTANZA

Il codice del consumo: linguaggio chiaro e comprensibile

Nell'ambito che ci interessa, parliamo di contratti a distanza quando essi vengono conclusi utilizzando il software con l'utilizzo dell'informatica. Bisogna prima distinguere i **contratti conclusi fuori dai locali commerciali**, dai **contratti a distanza**. I primi sono quelli che si possono concludere quando non avviene in un luogo commerciale, ma viene effettuato in presenza, nei contratti a distanza, invece, dove **non c'è una compresenza delle persone** c'è il rischio di concludere un contratto senza accorgersene. Il decreto legislativo del 2005, ovvero il **codice del consumo**, definisce una serie di diritti dei consumatori per disciplinare numerose situazioni nel nostro quotidiano da consumatori. Nel codice del consumo troviamo articoli che regolano i contratti a distanza. Queste regole sono lunghissime, complicate, rendendo faticoso mettere ordine a queste norme. Ci sono comunque degli aspetti interessanti per il contratto a distanza. Il tema che ci interessa è quello del contratto nel quale l'acquirente **non ha di fronte la persona, nemmeno virtualmente**. Uno degli aspetti fondamentali nei contratti a distanza è quello della necessità di un **linguaggio chiaro e comprensibile**. Chi acquista un prodotto o un servizio deve essere in grado di capire ciò che sta facendo. In particolare, per linguaggio chiaro e comprensibile, vuol dire che dall'altra parte la persona può non essere in grado di conoscere certe terminologie tecniche. Non bisogna quindi utilizzare concetti troppo difficili, rendendo quindi, come abbiamo già detto, la persona in grado di capire le azioni che sta compiendo.

Il diritto di recesso

Nei contratti a distanza vi è un elemento di protezione del consumatore assente nei contratti che si concludono presso la sede del professionista. Questa forma di protezione è il **diritto di recesso**. In Italia il recesso non c'è come regola, esclusi i casi in cui le leggi lo prevedono. Capita spesso che nel codice del consumo ci siano regole opposte a quelle del codice civile. Il codice civile va analizzato da un profilo economico dove i contratti previsti sono stabili, garantendo quindi una maggiore affidabilità nel momento della stipulazione di un contratto. Il punto di vista del codice del consumo è quello della protezione del consumatore che spinge il professionista ad adattarsi a meccanismi di trasparenza e chiarezza. Il diritto di recesso è un diritto **non rinunciabile**: questo evita al professionista di comportarsi in maniera sleale. Gli unici costi che sono a carico del consumatore in caso di recesso sono le **spese postali di spedizione** ed eventuali **costi che derivano dalla manipolazione del bene**. Per il diritto di recesso si usa la **mail box rule**: il consumatore esercita il recesso nel momento in cui la comunicazione è stata fatta partire, rovesciando così la regola del codice civile per la quale i diritti connessi alla comunicazione sono efficaci solo se essa arriva al domicilio. Ci sono eccezioni al diritto di recesso: beni alimentari, prodotti su misura, apertura dall'involucro del software (ormai obsoleto) e servizi eseguiti sono esempi validi su cui non si può applicare il diritto di recesso. Un esempio di servizio eseguito è l'assistenza da remoto.

Un esempio di servizio a distanza: il cloud computing

Uno dei campi in cui operano i servizi a distanza è sicuramente il **cloud computing**. Il cloud computing è un servizio offerto per il quale le regole possono essere trovate nel codice civile. Esiste un **obbligo di comportamento adeguato** che non è descritto nei contenuti e che andrà verificato in base allo stato della scienza esistente nel momento in cui un certo programma viene eseguito. L'adeguatezza della propria preparazione nel predisporre un software, **comporta la responsabilità per i danni che si cagionano**. Altro aspetto del cloud computing riguarda il deposito dei dati: dal punto di vista giuridico, che cos'è un file? Il codice civile parla di beni mobili quando essi sono ancorati alla loro fisicità: il file è un bene materiale o un bene immateriale? In generale le energie, quando hanno un valore economico, sono considerati beni mobili. Da questo punto di vista il file, essendo una scritturazione elettronica è un bene mobile. Qual è la disciplina nel codice civile sul deposito? I servizi di storage possono essere gratuiti o pagamento: la custodia dei dati è soggetta a **minor rigori in caso di gratuità** rispetto a un servizio a pagamento.

Le aste online

L'asta è una modalità particolare di scambio di beni o servizi che si avvale di un insieme di regole e strutture che permettono la **fissazione dinamica del prezzo**. La potenzialità più evidente dell'asta on-line è l'utilizzo di uno spazio virtuale e non più fisico, consentendo a persone dalle più svariate posizioni del pianeta di parteciparvi. I principali tipi d'asta sono 3.

Asta all'inglese: si parte da un'offerta minima rispetto alla quale i partecipanti possono rilanciare il prezzo fino alla scadenza del tempo prestabilito

Asta all'olandese: l'offerente offre un bene o un servizio al prezzo più alto, abbassandolo progressivamente fino a che un partecipante non accetta l'offerta

Asta al secondo prezzo: gli offerenti dispongono la loro offerta in una busta sigillata e simultaneamente la passano al banditore. Le buste sono aperte e l'individuo con la più alta offerta vince l'asta, pagando un prezzo pari al secondo ammontare offerto più alto.

Riassunto e approfondimenti

Commercio elettronico indiretto: fasi informative, documentali, contrattuali, regolazione finanziaria, svolte per via telematica. La consegna del bene invece è fisica.

Commercio elettronico diretto: come quello indiretto ma anche la consegna del bene è virtuale.

Diritto di recesso: nei servizi a distanza, si può effettuare senza penalità e senza specificarne il motivo, entro 14 gg lavorativi.

Consumatore: persona fisica che agisce con finalità non riferibili all'attività commerciale, imprenditoriale o professionale eventualmente svolta (altrimenti sarebbe un professionista).

Registri immobiliari: vicende di titolarità dei beni e della loro circolazione. Non sono basati sul catasto, sono impostati su base personale. I dati si cercano tramite il soggetto o l'immobile stesso. La **rigidità del linguaggio informatico per i registri immobiliari** è la difficoltà a far capire alle macchine alcune sfumature che a volte caratterizzano le fattispecie giuridiche.

GLI SMART CONTRACT

Smart contract come contratti vincolanti

Esiste una norma di legge che qualifica gli smart contract: l'**articolo 8 ter del decreto legge 135 del 2018**. Possiamo dire che si parla di smart contract quando **ricorrono le condizioni indicate dalla legge**. La definizione che troviamo: *si definisce smart contract, un programma per l'elaboratore che opera su tecnologie basate su registri distribuiti per i quali si realizza la tecnologia blockchain, la cui esecuzione vincola automaticamente due o più parti sulla base di effetti predefiniti*. Questa definizione molto ampia cerca di coprire varie situazioni ma può risultare difficile da comprendere: a quale obiettivo le parti si sono prefissate quando utilizziamo la tecnologia dei registri distribuiti? L'aspetto centrale dello smart contract non è la tecnologia: l'obiettivo è far capire che **se si verificano determinati presupposti, allora le parti sono vincolate**. Gli smart contract vincolano due o più soggetti, considerando **diverse variabili**. Un esempio banale è l'ammontare di denaro inserito in un distributore, ma le variabili in gioco possono essere molto più complesse e numerose. Ma il problema del diritto è che queste variabili non si possono ridurre a questioni deterministiche con consequenzialità: il diritto è una scienza umana, non una scienza esatta, ci sarà sempre un margine di incertezza ingovernabile. Quando si usano i registri distribuiti è necessaria l'attribuzione di una **data certa**, cioè un dato sicuro dal profilo giuridico, nel senso che non può essere alterato. Per attribuire certezza ad un documento ci sono due possibilità: la firma digitale con marca temporale oppure l'utilizzo di posta elettronica certificata. Inoltre, quando un documento viene immesso in una blockchain, la sua immodificabilità permette di assicurarci tranquillamente di attribuire una data certa a tale documento (timestamp o marca temporale automaticamente attribuita nel momento in cui un documento viene inserito in una blockchain). Gli smart contract possono avere un ambito di funzionamento anche in quei casi in cui si **rinuncia a far valere forme di protezione e tutela che il codice fornisce**. Possiamo quindi ridurre l'intervento del giudice passando dalla scienza umana a una scienza esatta, valutando costi benefici di questa rinuncia. In generale, il costo del malfunzionamento che porterà davanti al giudice lo si può distribuire con i guadagni raggiunti (possibile per le grandi imprese).

IL DIRITTO D'AUTORE

Il diritto d'autore: storia

La protezione del diritto d'autore è ormai conosciuto da tempo dal diritto. Con l'avvento dell'informatica il diritto d'autore ha subito una profonda trasformazione. Cominciamo col dire che c'è un'enorme dibattito tra la protezione del diritto d'autore e la libertà di utilizzare le invenzioni. Bisogna entrare in un'ottica di tipo economica: il frutto degli sforzi fatti viene riconosciuto oppure no? Tutti ne usufruiscono in ugual misura? Il diritto d'autore nasce nel 1710 con lo **statuto di Anna**, la prima legge sul copyright nel Regno di Gran Bretagna. Il problema fu posto ancora più indietro, quando Gutenberg inventò la stampa, o per meglio dire i caratteri mobili che consentirono la stampa di molti scritti in maniera industriale per il tempo di allora (ovvero 1400 - 1450). Qui nasce il primo **meccanismo di controllo**: il sovrano concede la stamperia a qualcuno e stampa solo ciò che viene accettato dal sovrano. Col passare del tempo la stampa sfugge dalle mani del sovrano. Ora il problema è che **chi crea un'opera vuole essere protetto**. Questa protezione sarà realizzata proprio dalla regina nel 1710.

Il diritto d'autore come forma di salvaguardia

La norma a protezione del diritto d'autore rappresenta quindi una forma di salvaguardia delle proprie opere, **anche quando non esiste uno sfruttamento economico immediato che è insito nelle invenzioni**. Ciononostante si è deciso di proteggere il software con le norme sul diritto d'autore e non con le norme sulle invenzioni. In Italia il diritto d'autore viene introdotto nel 1941 con **la legge numero 633 del diritto d'autore**. Nel 1941 non ci si poneva nemmeno il problema del software, anche se ci sono elementi utilizzati ancora oggi. La legge sul diritto d'autore non ci dice cos'è un'opera dell'ingegno, non vi è una definizione, ciò che viene richiesto è che ci sia un **aspetto creativo**, l'unica cosa che conta affinché ci sia la protezione del diritto d'autore è puramente e semplicemente la creatività (che potrebbe essere intesa anche come la creazione di qualcosa che ancora non c'è). Che tipo di protezione ci dà il diritto d'autore? Ci dà **2 forme di protezione**: una viene chiamata **diritto morale** e una viene chiamata **diritto di sfruttamento economico (patrimoniale)**. Il diritto morale è il diritto che ha l'autore di rendere pubblica la sua opera, di vietare che sia resa pubblica e di essere riconosciuto come autore della stessa. Questo diritto gli spetta per tutta la vita e alla sua morte spetta ai suoi discendenti in maniera indefinita. Il diritto di sfruttamento è il diritto di utilizzare la propria opera e di farne tutto il guadagno che quell'opera consegue. Mentre il diritto morale non si può vendere (in un certo senso consentirebbe di alterare la storia), il diritto di sfruttamento economico può essere venduto. Il diritto di sfruttamento si estingue dopo 70 anni dalla morte dell'autore.

Il diritto d'autore nell'informatica

Il file ha dei requisiti tali che consentono di immaginare utilizzi non previsti dal diritto d'autore: ci possono essere copie illimitate dei file senza distinzione dall'originale, la copia un file si trasmette facilmente e un file e le opere informatiche in generale possono avere meccanismi di criptazione. Tutto questo ha portato la necessità di modificare la legge sul diritto d'autore. Qual è uno dei primi problemi che pone la tecnologia? Che tipo di protezione viene dato all'autore, concretamente? La protezione del diritto d'autore è stata pensata per la fisicità e bisogna quindi tenere in conto l'aspetto immateriale dell'informatica. In contrapposizione a tutto ciò sono nati movimenti informatici che rivendicano la **libertà del software**, diventando così open source. Un esempio su tutti è Linux. Tuttavia, **il diritto morale rimane irrinunciabile**. Cosa succede se un programma originario subisce sostanziali modifiche? Chi ne diventa l'autore? In più cosa succede se il nuovo programma non aderisce alla politica open source? Ci sono una serie di complicate giuridiche a cui risulta difficile rispondere. Nel diritto privato, i beni gratuiti vedono una responsabilità molto ridotta, a meno che non si conoscano i difetti. Questo problema di responsabilità si attribuisce anche ai programmi open source. Spesso i programmi, come i sistemi operativi, hanno una **licenza d'uso**. La regola generale è che chi compra un bene ne diventa proprietario e ne faccia ciò che vuole secondo il **principio di esaurimento del diritto d'autore**. Il software non viene venduto così non c'è la pretesa di chiedere il codice sorgente. Con la licenza d'uso siamo in grado di utilizzarlo ma non di apprendere tutti i suoi contenuti. Tutti gli eventuali errori che si presentano sono quindi gestiti dal proprietario. La disposizione 64 bis della legge 633 protegge il programma ad ogni sua trasformazione.

Le banche dati

Un'altra forma di protezione inserita nel diritto d'autore sono le banche dati. Con le banche dati si trovano informazioni in poco tempo, permettendo quindi una ricerca immediata. Anche la banca dati è protetta dal diritto d'autore. Una banca dati si definisce tale se c'è un **linguaggio di interrogazione che consente la ricerca**: le banche dati sono quindi sono opere dell'ingegno.

Come proteggere gli autori?

Uno dei problemi che abbiamo finora lasciato sullo sfondo è come proteggere gli autori? Un file in senso ampio è facilmente copiabile in assenza di misure di protezione e facilmente trasmissibile. In ambito europeo, la direttiva 790 cerca di fare chiarezza anche sulla protezione del software: *gli Stati membri mettono in vigore le disposizioni legislative, regolamentari e amministrative necessarie per conformarsi alla presente direttiva entro il 7 giugno 2021*. Questa direttiva ha di importante l'articolo 17: esso regola l'utilizzo di contenuti protetti da parte di prestatori di servizi di condivisione di contenuti online. Viene comunque ribadito che **l'applicazione dell'articolo non comporta alcun obbligo generale di sorveglianza**. Ma allora come è possibile avvisare che ci sono opere protette dal diritto d'autore? Questo è un problema, poiché **i prestatori di servizio sono responsabili per atti non autorizzati al pubblico**, compresa la messa a disposizione del pubblico di opere e altri materiali protetti dal diritto d'autore, **a meno che non dimostrino di aver compiuto massimi sforzi per ottenere un'autorizzazione**.

Riassunto e approfondimenti

Opera dell'ingegno: non è definita dalla legge, ma la si può pensare come un'opera connessa a certi campi di produzione dell'ingegno umano.

Diritto d'autore e sampling: la protezione del diritto d'autore inizia nel XVIII secolo. Gli autori di un'opera dell'ingegno hanno diritto morale e patrimoniale d'autore. Sono tutelati anche gli autori che mettono "insieme i pezzi" (sampling, cioè incorporazione di più opere in una nuova opera, e remix) perché svolgono un'attività creativa e di progresso.

Plagio: appropriazione tramite copia totale o parziale della paternità di un'opera dell'ingegno altrui.

Esaurimento del diritto d'autore: avviene quando il bene protetto è stato messo in vendita la prima volta. Infatti, la prima vendita di una copia di un'opera protetta esaurisce il diritto di controllare l'ulteriore distribuzione sulla medesima copia.

Liceità dei videoregistratori: la liceità (ammissibilità) dei videoregistratori negli USA è stata ammessa perché essi permettono di fare cose illegali (copie in casa) ma anche di fare cose legali, nella maggior parte dei casi.

Licenza d'uso di un software: l'acquirente non acquista la proprietà del software, ma solo il diritto di usarlo per la sua attività commerciale, uso che è solitamente limitato al diritto di installazione su determinate macchine, alla visualizzazione e l'esecuzione del programma per lo scopo previsto dalla licenza. Tutti gli altri diritti restano in capo al venditore del software, quindi la possibilità di rivenderlo, copiarlo, modificarlo eccetera. L'acquirente della licenza d'uso non avrà mai la disponibilità del codice sorgente e quindi non potrà autonomamente gestire o modificare le funzionalità del software. La licenza d'uso può essere concessa a tempo indeterminato, tramite il pagamento di una cifra una tantum, o dietro pagamento di un canone annuale.

Vendita di un software: vengono ceduti tutti i diritti patrimoniali sul software, che il proprietario potrà usare a suo piacimento, caricarlo su supporti hardware, modificarlo e implementarlo, cederlo ad altri acquirenti. Avrà la piena disponibilità del codice sorgente.

LE MONETE E I MEZZI DI SCAMBIO VIRTUALI

Le prime forme di scambio

Il primo meccanismo con cui venivano scambiati beni era il **baratto**: ciò che conta è il valore che l'individuo attribuisce a ciò che dà e a ciò che riceve. A un certo punto della storia si è cominciato ad attribuire valore a oggetti di uso non immediato. L'oro, per esempio, è stato considerato fin dall'antichità un bene appetibile, raro che ha dato luogo al fenomeno della moneta. La storia della moneta vede nel tempo crearsi la **cartamoneta** che letteralmente non è altro che un pezzo di carta emesso da un'autorità centrale. Quando un'economia è forte in generale, ciò corrispondeva alla capacità dello Stato di avere tanto oro da permettersi di comprare tutti i dollari in circolazione, quando in economia è debole, allora lo Stato non ha oro a sufficienza a tale scopo: di conseguenza le banconote non valgono più nulla. In realtà non esistono più oggi depositi d'oro in quantità tale da garantire il valore della moneta. Oggi la forza di un'economia deriva dalla capacità di acquisto dello Stato derivanti dalla ricchezza che ha in modo da garantire il valore della moneta. Nel 1970 il presidente Nixon decise che il dollaro dovesse slegarsi dalla convertibilità in oro, acquisendo così una nuova forza. Nello stesso periodo, l'Arabia Saudita permise l'acquisto del petrolio con il solo utilizzo del dollaro.

Carte di credito e carte di debito

In tutti questi discorsi c'è stato dietro la fisicità. Inizialmente le carte di credito erano fortemente ancorate alla fisicità, senza alcun meccanismo di verifica: la banca doveva dare garanzie ai commercianti che accettavano i pagamenti attraverso carta di credito. L'informatica, quindi, ha consentito di verificare immediatamente se un'operazione eseguita con una carta di credito fosse coperta. La carta di credito promette di avere un credito, cioè una banca da la possibilità di spendere del denaro fino a una certa cifra. Con la carta di debito è permesso l'uso di capitale finanziario che non è di proprietà della banca ma del soggetto titolare della carta stessa.

La moneta elettronica

Per quanto riguarda la moneta elettronica essa riguarda più aspetti. Da un punto di vista giuridico con moneta elettronica ci si riferisce a quegli strumenti di pagamento in cui **non c'è più la moneta fisica**. Da questo concetto è nato anche l'**home banking**, cioè pagamenti effettuati da casa (una conseguenza è stata la riduzione degli sportelli bancari). Chi riceve soldi in contanti, a differenza delle transazioni eseguite per mezzo dei servizi bancari, non è tracciabile. Ci troviamo di fronte al **problema dell'anonimato**, cioè la circolazione della moneta è in forma anonima. Si è cercato di porre dei limiti alla circolazione del contante: più alto è il limite più risulta facile evadere le imposte, a differenza di pagamenti tracciati. La moneta di per sé è anonima.

Le criptovalute

Cerchiamo ora di dire qualcosa sulle criptovalute. Bitcoin ed Ethereum sono solamente due delle molte in circolazione. Da dove nasce il fenomeno delle criptovalute? Nasce da Satoshi Nakamoto (nessuno sa se sia una persona o un gruppo) che inventò utilizzando la tecnologia blockchain il sistema dei Bitcoin. L'aspetto fondamentale è che siamo di fronte a una serie di operazioni, unità in blocchi che si realizzano solamente da quando sono convalidate da almeno la metà più uno dei computer della rete e che danno vita al registro di queste operazioni. La tecnologia blockchain è stata studiata dalle banche centrali in quanto ci si è resi conto che la sua sicurezza risulta essere superiore a qualsiasi strumento in circolazione. Il sistema delle criptovalute è molto rischioso. Prima di tutto qual'è il valore del Bitcoin e delle monete virtuali in generale? In fondo dietro questa moneta non c'è alcuna economia. Il valore del Bitcoin, per esempio, viene attribuito semplicemente dando Bitcoin o frazioni di essi in mano ai minatori: per aggiungere una transazione alla blockchain è necessario crittografarla e convalidarla con una funzione di hash che richiede calcoli lunghi e complessi; quando il miner completa una transazione, una certa frazione di Bitcoin gli viene accreditata. Non esiste una convertibilità dei Bitcoin e non esiste un'autorità centrale che regola il valore di essi, il suo valore è **estremamente volatile** e per convertire il Bitcoin è necessario trovare degli acquirenti disposti a comprare beni o servizi acquistabili con essi. Quindi, a differenza delle monete legali nessuno risulta obbligato ad accettarli. Il mercato dei Bitcoin è **puramente finanziario**, cioè non è un mercato basato sullo scambio di merce ma sulle scommesse: tali mercati sono anche chiamati **speculativi**. Un'altro problema del Bitcoin è l'anonimato.

La moneta virtuale secondo l'Unione Europea

Una **direttiva dell'Unione europea del 30 maggio 2018** ha tra i considerando: *l'anonimato delle valute virtuali ne consente il potenziale uso improprio per scopi criminali. Le valute virtuali non vanno confuse con la moneta elettronica. Questo direttiva ci dice anche cosa si intende per valuta virtuale: una rappresentazione di valore digitale che non è emessa o garantita dalla Banca centrale o ente pubblico, non è necessariamente legata a una valuta legalmente istituita, non possiede lo stato giuridico di valuta o moneta, ma è accettata da persone fisiche o giuridiche come merce di scambio.*

Unità di conto virtuale

Con le recenti crisi economiche si è cominciato a parlare di **unità di conto virtuale**. Questa unità di conto non è una moneta regolamentata sul mercato, non è soggetto a speculazioni, ma è un'unità di conto con l'obiettivo di aiutare le imprese attraverso compravendite utilizzando l'unità stessa. Si basa sulla fiducia tra le imprese che, a fronte di un prestito di questa unità, sarà necessario ripagare con moneta reale. Questo concetto è nato in Sardegna nel 2008 con il nome di **Sardex**. Sulla fiducia di una disponibilità di una moneta che non esiste, che viene prestata a tutti e che tutti poi rimborsano, le imprese possono crescere aiutandosi tra loro. Ci troviamo quindi in una situazione dove **la moneta non è più usata per fini speculativi**.

Riassunto e approfondimenti

Criptovaluta: rappresentazione digitale di valore basata sulla crittografia.

Bitcoin: il Bitcoin è una moneta virtuale bidirezionale cioè convertibile in soldi veri, a differenza di altre monete virtuali. I Bitcoin vengono creati come **file criptati** creati da pc che usano certi software open source e vengono generati ed usati come forma di ricompensa attraverso il processo di mining.

Monete virtuali: Sardex e Venetex sono monete complementari (**strumenti di commutazione**, usati da certe comunità, **con cui è possibile scambiare beni e servizi affiancando il denaro ufficiale**) usate da imprese Italiane che hanno aderito al circuito per scambiarsi beni/servizi con altre imprese aderenti. Venetex è stato acquisito da Sardex.

Bruzio: coniato dal comune di Cosenza, è una moneta fisica da 20 euro data ai poveri al posto di sussidi economici (es. buoni spesa). I negozi la accettano e poi la convertono in euro.

REATI INFORMATICI

Che cosa si intende per reato?

Dobbiamo prima dare alcune indicazioni sul termine reato. Il termine reato si riferisce ad un comportamento per il quale **una legge penale applica una sanzione penale**. Non ci sono problemi a individuare queste leggi, poiché si usano termini tecnici ben chiari che fanno capire che si sta parlando di reato: **reclusione** o **arresto** (ovvero privazione della libertà personale), **multa** o **ammenda**. Non a caso, nel momento in cui si effettua un divieto di sosta non si troverà la parola multa nel documento. Il vigile non può infliggere una multa: le sanzioni penali sono inflitte solo ed esclusivamente da un giudice e a seguito di un processo. Il codice penale è formato da 3 libri: uno riguarda le disposizioni generali su cosa sono i reati, uno colpisce i delitti, cioè reati più gravi, e uno colpisce le contravvenzioni, cioè reati meno gravi. Ci sono alcuni **principi fondamentali del diritto penale**: ciascuno risponde esclusivamente dei propri comportamenti, la legge che prevede un reato deve necessariamente essere commessa prima del fatto che viene incriminato (cioè **non è possibile avere una legge retroattiva**) e le norme penali sono **tassative**, cioè valgono esclusivamente per i casi previsti dalla regola. Commettere reati più volte fa della persona un **delinquente per tendenza** o abituale. Le sanzioni penali sono iscritte nel casellario giudiziario. Alcuni reati sono punibili a **querela di parte**: la querela è la richiesta di chi ha subito il reato (il danneggiato) di chiedere al giudice di punire colui che lo ha commesso. Se non si fa la querela entro tre mesi da quando è successo il fatto il reato si estingue, ovvero è **improcedibile** l'azione penale. Tutti gli altri reati sono **perseguibili d'ufficio**, cioè non serve la querela. Un'altro aspetto in termini di reati è la differenza tra **dolo** e **colpa**. Dolo vuol dire commettere volontariamente un reato. La colpa è una commissione volontaria di reato. Le contravvenzioni sono punite sia se dolose che colpose. I delitti sono solo dolosi, salvo quelli in cui testualmente indicato anche colposi. Queste sono le istruzioni minime che ci aiutano ad entrare nel termine di reati informatici. L'ultima cosa da sapere è che **le norme penali italiane raramente prevedono la sanzione precisa**: la sanzione va da un minimo a un massimo, perché il giudice deve valutare una serie di comportamenti.

I reati informatici

Quando parliamo di reati informatici distinguiamo i **reati che riguardano i mezzi informatici**, dove il mezzo è la vittima e i **reati commessi per mezzo dell'informatica**. Un esempio è l'utilizzo indebito delle carte di credito, dove l'informatica entra solo perché parliamo di strumenti elettronici. Alcuni reati informatici sono indicati nel codice penale.

- Art. 392 c.p.: **Esercizio arbitrario delle proprie ragioni con violenza sulle cose**

Chiunque, al fine di esercitare un preteso diritto, potendo ricorrere al giudice, si fa arbitrariamente ragione da sé medesimo, mediante violenza sulle cose, è punito, a querela della persona offesa, con la multa fino a euro 516. Agli effetti della legge penale, si ha violenza sulle cose allorché la cosa viene danneggiata o trasformata, o ne è mutata la destinazione. **Si ha altresì, violenza sulle cose allorché un programma informatico viene alterato, modificato o cancellato in tutto o in parte ovvero viene impedito o turbato il funzionamento di un sistema informatico o telematico.**

- Art. 495-bis c.p.: **Falsa dichiarazione o attestazione al certificatore di firma elettronica sull'identità o su qualità personali proprie o di altri**

Chiunque dichiara o attesta falsamente al soggetto che presta servizi di certificazione delle firme elettroniche l'identità o lo stato o altre qualità della propria o dell'altrui persona è punito con la reclusione fino ad un anno.

- Art. 615-ter c.p.: **Accesso abusivo ad un sistema informatico o telematico**

Chiunque abusivamente si introduce in un sistema informatico o telematico protetto da misure di sicurezza ovvero vi si mantiene contro la volontà espressa o tacita di chi ha il diritto di escluderlo, è punito con la reclusione fino a tre anni. La pena è della reclusione da uno a cinque anni: se il fatto è commesso da un pubblico ufficiale o da un incaricato di un pubblico servizio, con abuso dei poteri; se il colpevole per commettere il fatto usa violenza sulle cose o alle persone, ovvero se è palesemente armato; se dal fatto deriva la distruzione o il danneggiamento del sistema.

- Art. 615-quater c.p.: **Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici**

Chiunque, al fine di procurare a sé o ad altri un profitto o di arrecare ad altri un danno, abusivamente si procura, riproduce, diffonde, comunica o consegna codici, parole chiave o altri mezzi idonei all'accesso ad un sistema informatico o telematico, protetto da misure di sicurezza, o comunque fornisce indicazioni o istruzioni idonee al predetto scopo, è punito con la reclusione sino ad un anno e con la multa sino a euro 5.164.

- Art. 615-quinquies c.p.: **Diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico**

Chiunque, allo scopo di danneggiare illecitamente un sistema informatico o telematico, le informazioni, i dati o i programmi in esso contenuti o ad esso pertinenti ovvero di favorire l'interruzione, totale o parziale, o l'alterazione del suo funzionamento, si procura, produce, riproduce, importa, diffonde, comunica, consegna o, comunque, mette a disposizione di altri apparecchiature, dispositivi o programmi informatici, è punito con la reclusione fino a due anni e con la multa sino a euro 10.329.

- Art. 617-quater c.p.: **Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche**

Chiunque fraudolentemente intercetta comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi, ovvero le impedisce o le interrompe, è punito con la reclusione da sei mesi a quattro anni.

- Art. 621 c.p.: **Rivelazione del contenuto di documenti segreti**

Chiunque, essendo venuto abusivamente a cognizione del contenuto, che debba rimanere segreto, di altrui atti o documenti, pubblici o privati, non costituenti corrispondenza, lo rivela, senza giusta causa, ovvero lo impiega a proprio o altrui profitto, è punito, se dal fatto deriva nocumento, con la reclusione fino a tre anni o con la multa da euro 103 a euro 1.032.

- Art. 635-bis c.p.: **Danneggiamento di informazioni, dati e programmi informatici**

Salvo che il fatto costituisca più grave reato, chiunque distrugge, deteriora, cancella, altera o sopprime informazioni, dati o programmi informatici altrui è punito, a querela della persona offesa, con la reclusione da sei mesi a tre anni. Se il fatto è commesso con violenza alla persona o con minaccia ovvero con abuso della qualità di operatore del sistema, la pena è della reclusione da uno a quattro anni.

IL CODICE DELL'INFORMATICA

Le regole nell'informatica: la mancanza di un codice specifico

Ciò che caratterizza il diritto dell'informatica è la **mancanza di un codice**, di un corpo uniforme di regole. Dove si trovano i principi generali che ci consentono di dire quali sono le regole fondamentali entro i quali ci si deve muovere? Spesso è necessario estendere le regole vigenti alle situazioni in cui entra in gioco il mezzo informatico con un **meccanismo di adattamento**. Un codice abbastanza conformato alle esigenze di oggi è il **codice delle telecomunicazioni**, cioè il decreto legislativo numero 259 del 2003, che ha subito una forte modifica nel 2012. Chi è che governa la materia delle telecomunicazioni? Il problema è che le amministrazioni al vertice hanno soggetti politici: i ministri che effettuano le scelte. Per fare in modo che queste scelte siano il più possibile meno politicizzate, assumendo una sorta di oggettività, a partire dagli anni 90 si è previsto di creare dei soggetti che sono indipendenti, chiamati autorità indipendenti che non rispondono né al governo né al suo indirizzo politico. In particolare i soggetti di riferimento sono il **ministero delle comunicazioni** e l'**autorità delle telecomunicazioni**, senza dimenticarci delle regole per capire quali sono i nostri diritti e i nostri obblighi.

Il codice delle telecomunicazioni

Quali sono i principi generali che troviamo nel codice delle delle comunicazioni? L'articolo 3 (principi generali) dice: *il codice garantisce i diritti inderogabili di libertà delle persone nell'uso nel mezzo di comunicazione elettronica, nonché il diritto di iniziativa economica su esercizio di regime di concorrenza*. Ciò si discosta dal regime di regole precedenti a tale codice, dove tutto l'esercizio delle comunicazioni era nelle mani del ministro: ciò non vuol dire che non ci siano controlli nelle comunicazioni, c'è la necessità di sicurezza per evitare situazioni di pericolo. Sempre nell'articolo 3 si esprime che la fornitura di reti e servizi di comunicazione elettronica è libera. Si ribadisce poi il concetto di net neutrality, garantendo il rispetto del principio di neutralità tecnologica inteso come non discriminazione tra particolari tecnologie, non imposizioni nell'uso di una particolare tecnologia e possibilità di adottare provvedimenti ragionevoli al fine di promuovere i servizi indipendentemente dalla tecnologia utilizzata. Nel codice troviamo poi diritti di **libertà di comunicazione, segretezza delle comunicazioni, libertà di iniziativa economica sul regime di concorrenza**. La libertà di concorrenza in Italia comincia a trovare delle regole importanti nel 1990. In termini di comunicazione è fondamentale la concorrenza perché permette **miglioramenti del prodotto e del servizio e abbassamento dei prezzi**: il monopolio viene quindi guardato con sfavore. L'articolo 16 del codice: *le imprese che detengono diritti esclusivi o speciali esercitati in Italia o all'estero, anche a livello locale, non possono fornire reti o servizi di comunicazione elettronica accessibile al pubblico, se non attraverso società controllate*. Sempre in tema di libertà di concorrenza, *l'attività di fornitura di reti e servizi è libera e assoggettata ad un'autorizzazione generale che consegue alla presentazione della domanda*. **L'attività di installazione delle reti è quindi libera**, con dovuti controlli sulle interferenze. Inoltre, l'articolo 89 dice che *l'autorità, anche mediante l'adozione di specifici regolamenti, può imporre la condivisione di infrastrutture nel pieno rispetto del principio di proporzionalità*. Nell'articolo 90 del codice delle telecomunicazioni si dice che *gli impianti e le opere accessorie di uso privato possono essere dichiarati di pubblica utilità con decreto del Ministro dello Sviluppo economico*. A questo punto tale attività viene attratta all'interno di regole che riguardano **l'espropriazione per pubblico interesse**. È possibile quindi invadere la proprietà privata scardinando la regola fondamentale in materia di proprietà: *il proprietario o il condominio non possono opporsi all'appoggio di antenne di sostegno, nonché il passaggio di condutture, fili o qualsiasi altro impianto occorrente per soddisfare le richieste di utenza degli inquilini o dei condomini*. Quindi gli articoli 90 e 91 fanno **prevalere l'interesse delle imprese e quello collettivo all'interesse individuale**.

Il diritto dell'informatica nel mondo

Poiché le attività poste in essere sulla rete oltrepassano il confine degli Stati, alcuni sostengono che è necessario ricorrere agli strumenti del diritto internazionale per disciplinare tale attività. Si pensi, ad esempio, alla **Convenzione sul cybercrime**, elaborata dal Consiglio d'Europa, nel 2001, e ratificata in Italia, nel 2008, la quale costituisce il primo trattato internazionale sui reati via Internet, che si occupa di violazione del copyright, delle frodi telematiche, della pedofilia, e degli attentati all'integrità delle reti, e che mira a perseguire una politica criminale comune contro il cybercrime, adottando una legislazione adeguata, e favorendo la cooperazione internazionale.

NOMI DI DOMINIO

Il marchio

Il nome di dominio è un indirizzo IP che, anziché essere espresso in numeri, viene espresso in parole: è un sistema comodo ed efficiente per essere riconosciuti nella rete. Se vediamo il nome di dominio da un punto di vista imprenditoriale, esso distingue il soggetto da altri, i quali non devono appropriarsi di esso o fare attività in grado di creare confusione. Nel diritto della concorrenza questa disciplina era riferita ai marchi e alla ditta, che sarebbe il nome dell'imprenditore. Registrare un marchio significa averne il suo utilizzo esclusivo e di impedire ad altri di utilizzarlo. Per i nomi di dominio succede un po' la stessa cosa. Ci sono in particolare due situazioni: la **contraffazione** e la **confusione**. La contraffazione è la copia illecita di un marchio, che cagiona un danno gravissimo. Ci sono poi marchi che assomigliano più che al nome al disegno, generando quindi confusione. Anche nei marchi vale il diritto d'autore, dove si chiede nel marchio una certa originalità e capacità distintiva. La legge protegge il titolare del marchio sia dalla contraffazione che dalla confusione. Tutto ciò è disciplinato a partire dalla regolamentazione degli uffici che registrano i marchi e i brevetti in base a delle norme che prevedono come si debba fare e quali sono le capacità distintive. Ci sono anche convenzioni internazionali ai fini della protezione: a una multinazionale interessa difendere i suoi tratti distintivi in tutto il mondo, non solo in una realtà locale.

Il nome di dominio

Il nome di dominio assomiglia molto a un marchio: è il **sistema che identifica un certo sito**. È poi possibile utilizzare il nome del marchio come il nome di dominio, collegandolo poi ai prodotti. Qui troviamo gli stessi fenomeni del marchio che si traducono in **cybersquatting** e **typosquatting**. Il cybersquatting è l'appropriazione di nomi di domini corrispondenti a marchi commerciali altrui o a nomi di personaggi famosi al fine di realizzare un lucro, mentre il typosquatting è una forma di cybersquatting e consiste nello sfruttare errori di battitura per dirottare l'utente verso un sito differente da quello che voleva raggiungere (per esempio google e goggle). Ma chi è che decide dei nomi di dominio? Esiste il **regolamento per l'assegnazione di dei nomi di dominio**, per il quale però non si capisce la natura giuridica del soggetto che l'ha creato, ovvero **Registro.it**. Se cercassimo una norma che ci consente di dare un inquadramento giuridico alla gestione dei nomi di dominio, troveremmo solo l'articolo 15 del codice delle telecomunicazioni che dice: *il ministero delle Telecomunicazioni vigila sull'assegnazione dei nomi di dominio e indirizzamento*. Stiamo sempre parlando di una norma vaga in quanto si tratta di **vigilanza**: chi decide dei nomi di dominio? Come funziona il meccanismo non ci viene detto.

DOMANDE FINALI

Cos'è il diritto?

Insieme di comandi/ordini imposti da un'autorità con un potere attribuitogli dalla costituzione.

Cos'è il diritto dell'informatica?

L'insieme di tutti i regolamenti che riguardano il rapporto delle persone con e attraverso sistemi informatici. Non esiste un codice unico data l'ampiezza dell'argomento e del cambiamento continuo

Quali sono le 2 tipologie di sanzioni?

Penale: inflitta da un giudice e comporta conseguenze gravi. Amministrativa: in genere solo di natura pecuniaria e non inflitta da giudici

Cos'è la Neutralità della Rete?

È il principio secondo il quale l'accesso alla rete non deve discriminare la persona, o il dispositivo utilizzato per accedere ad essa. Citato in molti documenti anche dell'unione europea ma non ancora completamente fatta valere / imposta.

Quale fu il primo testo di legge italiano che prese in considerazione la tecnologia digitale?

Imporre alle pubbliche amministrazioni di fare uso delle nuove tecnologie: codice dell'amministrazione digitale.

Cos'è un documento informatico?

Un file di solito di tipo .pdf creato usando una funzione di hash e con collegata una chiave asimmetrica che rappresenta la firma digitale dell'autore. Se questo documento venisse modificato, l'hash verrebbe invalidato automaticamente.

Cos'è la posta elettronica e la PEC?

Un metodo di scambio di informazioni, sostanzialmente la digitalizzazione della posta tradizionale, la PEC, ovvero Posta Elettronica Certificata è una tipologia di casella di posta certificata e firmata, utilizzando gli stessi sistemi del documento informatico e con ulteriori funzioni e protezioni, come ad esempio la conferma di ricezione ha validità legale.

Cos'è la tecnologia Blockchain?

Meccanismo tecnologico organizzato come catena di blocchi, che registra ogni operazione fatta su di essa. È la base delle criptovalute ed una delle strutture informatiche più sicure al mondo, dato che è basata sulla potenza di calcolo complessiva dell'intero sistema connesso alla catena.

Cosa sono le monete virtuali / elettroniche?

La carta moneta, il cui valore era in passato basato strettamente sul valore di una materia prima come l'oro, ad oggi si basa invece sull'economia di un paese. Il problema intrinseco delle monete fisiche è la natura non tracciabile ed il conseguente uso per operazioni illecite, per questo si introduce la moneta elettronica come strumento di pagamento caratterizzato dall'assenza di fisicità della moneta ma dalla presenza di un meccanismo elettronico che dà disposizione dei fondi, interamente tracciabile. Con la tecnologia blockchain si introducono delle valute alternative che offrono vantaggi e svantaggi: sono molto più sicure dato che sono basate su blockchain ma pericolose perché instabili (non essendo collegate ad un valore reale) e non tracciabili (tornando quindi al problema della moneta fisica) queste valute alternative sono chiamate valute virtuali, ovvero una rappresentazione di valore digitale che non è emessa o garantita da una banca centrale o da un ente pubblico, non è necessariamente legata ad una valuta legalmente istituita, non possiede lo status giuridico di valuta o moneta ma è accettata da persone come mezzo di scambio.

Che cambiamenti ci sono stati per quanto riguarda i contratti?

Nascono gli smart contract come tipologie di contratti con elementi attivabili immediatamente. La possibilità di firmare contratti a distanza senza comunicazione diretta fra persone. Elementi di protezione del consumatore aggiuntivi come il diritto di recesso, ovvero la possibilità di ritirarsi dal contratto anche dopo averlo firmato ammettendo eccezioni come: prodotti in scadenza (alimentari), prodotti su misura, software su licenza fisica (CD), servizi già usufruiti / eseguiti (assistenza remota)

Cosa sono gli Smart Contract?

Un tipo di contratto contenente elementi attivabili automaticamente una volta sottoscritto, esempio: macchinette del caffè o del parcheggio.

Come veniva trattata la privacy prima dell'era digitale?

Prima dell'avvento del digitale, c'erano pochi regolamenti riguardanti la riservatezza perché era molto più difficile violare la privacy di una persona nello stesso modo che le nuove tecnologie ci permettono

Cos'è un dato sensibile?

Per dati sensibili si intende una particolare categoria di dati delicati : origine razziale ed etnica, convinzione religiose, filosofiche, opinioni politiche, partiti sindacati, salute e vita sessuale.

Cos'è il diritto all'oblio?

La non diffusione di informazioni, solitamente giudiziarie, che potrebbero compromettere la vita di una persona

La raccolta dati è opzionale?

Se possibile, la raccolta dati deve essere assente o come minimo anonima e temporanea. Solo nei casi in cui è strettamente necessario si può non rispettare questi limiti, avvisando chiaramente l'utente della memorizzazione dei propri dati

Che regolamenti ci sono riguardo i Social Network e come funzionano?

I Social Network sono dei servizi offerti da degli internet provider NON responsabili del contenuto caricato dagli utenti. Questi servizi sono solitamente gratuiti perché la profilazione dell'individuo e la conseguente vendita di tali informazioni è sé stesso il pagamento, spesso come aggiunta o alternativa si fa uso di pubblicità per recuperare i costi

Cos'è il Commercio Elettronico?

È caratterizzato dall'assenza del contatto fisico in favore dell'utilizzo di internet, è sopportato in gran parte grazie alle pubblicità televisive o internet. Per legge non può essere ostacolato a favore del Commercio Tradizionale e viceversa ad esempio attraverso tasse aggiuntive o tasse elevate. Il trasportatore non è responsabile del contenuto.

Come è cambiato il diritto d'autore con l'avvento delle nuove tecnologie?

Nel diritto si distinguono le opere dalle invenzioni, le prime sono frutto di creatività e vengono protette a prescindere dal loro eventuale utilizzo economico, le invenzioni invece non sono sempre protette data la loro natura prettamente economica e non creativa. Il software viene individuato come un'opera creativa, perciò protetta dal diritto d'autore. I diritti dell'autore sono quello morale (diritto di pubblicizzare l'opera, di esserne riconosciuto l'autore sempre e di opporsi a qualsiasi tipologia di deformazione o modificazione apportata da terzi) e patrimoniale (diritto di essere ricompensato per la vendita dell'opera, esaurito dopo la prima vendita, in quanto potrà essere rivenduto più volte senza ricompensare l'autore. Si estingue dopo 70 anni dalla morte dell'autore). Le nuove tecnologie hanno portato a movimenti contro il diritto d'autore, come ad esempio il codice open source, composto spesso da collaborazioni di sviluppatori che rinunciano al diritto d'autore a favore dello sviluppo continuo e collaborativo di più persone per migliorare di continuo il prodotto. Nel caso di software, l'utente finale compra una licenza di utilizzo, non il software in sé, perché altrimenti per legge avrebbe il diritto di accesso al codice sorgente.

Cosa sono i reati informatici?

Tutti i reati caratterizzati da danni effettuati attraverso l'utilizzo di sistemi informatici o danni effettuati ad un mezzo informatico come malware apposti per la raccolta di dati da un dispositivo (registratori), intercettazione di comunicazioni, cyberbullismo, accesso Abusivo di un sistema protetto, diffusione di codici di accesso a sistemi protetti, rivelazione del contenuto di documenti segreti, frode informatica, malware apposti per il blocco di un dispositivo e la successiva estorsione del proprietario, diffusione di apparecchiature dirette al danneggiamento di un sistema informatico.

Cosa sono le aste informatiche?

Aste effettuate attraverso l'utilizzo di internet come mezzo di comunicazione

Come vengono gestite le infrastrutture di rete?

Rappresentano un potenziale monopolio di fatto dato l'alto costo e devono perciò poter essere condivise laddove possibile.

Cosa sono i nomi di dominio?

Associano un nome ad un indirizzo IP di un server, vengono considerati come un'estensione del marchio e come tale è soggetto a protezioni. Non esistono discipline legali sull'assegnazione dei nomi di dominio.

DOMANDE RAPIDE FINALI

Esiste una disciplina legale dei nomi di dominio?

No, esistono regole sporadiche.

Cosa si intende per principio di neutralità della rete?

Che chi opera nella rete non deve discriminare tra tecnologie di accesso.

Quando in Italia la riservatezza è divenuta diritto tutelato dalle leggi?

A metà degli anni 90.

Perché di solito un internet provider non chiede un canone all'utente?

Perché vende le informazioni sugli interessi dell'utente.

Un file è un documento valido?

Sì.

Cosa è la dematerializzazione dei titoli finanziari?

Il fatto che i titoli di carta sono stati sostituiti da scritturazioni elettroniche.

Cosa è l'informatizzazione dei registri immobiliari?

Il fatto che i registri di carta sono ora digitali.

I bitcoin sono una moneta?

No, sono un mezzo di scambio.

Il commercio elettronico riguarda?

Consumatori e/o imprese.

Per effettuare una comunicazione commerciale?

Occorre che chiariscano di essere comunicazioni commerciali.

A cosa servono i marchi di qualità?

Per acquistare la fiducia dei clienti sulla bontà del prodotto.

Si possono utilizzare tecniche digitali per bloccare l'accesso a proprie opere dell'ingegno?

Si sempre.

Esistono norme penali contro l'uso improprio del software?

Si e riguardano anche i mezzi di pagamento elettronico.

I providers devono controllare il materiale che viene inserito dagli utenti?

No.

Quali regole disciplinano i social network?

Il contratto ed eventuali norme di legge.

Quando un file contiene un valido documento?

Quando viene sottoscritto digitalmente.

La posta elettronica certificata?

È l'unica che attribuisce certezza di provenienza dei messaggi.

È obbligatorio possedere la pec?

Si per alcuni soggetti.

Cos'è una firma elettronica avanzata?

La possibilità di individuare legalmente il firmatario del documento.

Cos'è il principio di neutralità della rete?

La necessità che la rete non discrimini tra mezzi tecnologici.

Chi è il consumatore?

Chiunque compri beni per scopo personale.

I servizi delle società dell'informazione sono regolati?

Solo quando resi a pagamento

Come è definita un'opera dell'ingegno?

La legge non la definisce.

Cosa si intende per sampling?

L'incorporazione di più opere in una nuova opera.

Cosa si intende per cloud computing?

Una serie di positivi resi mediante icloud.

Cosa si intende per commercio elettronico indiretto?

Il commercio in cui l'informatica è solo un mezzo di comunicazione.

Esiste un codice di diritto dell'informatica?

No.

Dove si trovano le regole sulla trasparenza nelle comunicazioni elettroniche?

Nel codice delle telecomunicazioni.

Cosa si intende per privacy?

Il diritto di mantenere il controllo sulle proprie informazioni.

Si può imporre ad un'amministrazione di rispondere via pec alle istanze dei privati?

Sì.

Quando non si adottano misure minime di sicurezza nella conservazione dei dati vi è una responsabilità?

Penale.

Cosa è il processo civile telematico?

Il processo civile in cui il deposito degli atti avviene in forma telematica.

Quando un documento inviato a mezzo posta certificata si considera consegnato?

Quando arriva al server del destinatario.

Cosa è la dematerializzazione dei titoli?

Che i titoli cartacei sono stati sostituiti da registrazioni elettroniche.

Il commercio elettronico disciplinato dal codice del consumo vale?

Per le transazioni con strumenti telematici tra consumatori e imprese.

In caso di acquisti online si può recedere dall'acquisto?

Per le transazioni con strumenti telematici tra consumatori e imprese.

Il commercio elettronico disciplinato dalla disciplina delle società dell'informazione riguarda?

Qualsiasi transazione effettuata con strumenti telematici con imprese.

Cliccando su accetto sull'iscrizione ad un social network si conclude un contratto?

Si.

Da quando è la legge scritta a tutelare la privacy?

Dagli anni 90.

Chi è "responsabile" nel trattamento dei dati personali?

Chi è il titolare delle modalità di trattamento.

Le regole del codice dell'amministrazione digitale sui documenti informatici valgono per i privati?

Si.

Quali mezzi di comunicazione hanno la data certa opponibile a tutti?

La pec.

Si possono fornire ai consumatori beni non richiesti?

No occorre un previo ordine di acquisto.

Le banche dati sono tutelate?

Si sempre

Esiste un'autorità centrale che governa internet?

No.

I privati possono raccogliere i dati personali altrui?

Si ma solo se non sono destinati alla diffusione.

I documenti informatici?

Sono validi se con firma digitale.

Cos'è il fascicolo telematico?

Il fascicolo digitale del processo civile.

Che cosa è un wireless community network?

Un insieme di persone che crea una rete di comunicazioni wireless.

A cosa servono i marchi di qualità?

Informano l'acquirente sull'adempimento del venditore.

A cosa servono i marchi di qualità?

È una dichiarazione di un terzo circa l'affidabilità di un soggetto.

I bitcoins hanno valore stabile?

Tendenzialmente no.

Quando inizia il trattamento dei dati personali?

Da quando l'interessato rilascia il consenso.

I codici di autoregolazione sono obbligatori?

No

Scannerizzo ed appongo la mia firma ad un documento questa è una firma elettronica avanzata? OK

No

Si può concludere un contratto via mail?

Si.

Nei contratti a distanza con il consumatore questi può recedere?

Si senza dare spiegazioni.

Se compro un pc ed il software è in licenza?

Il software non è mio.

Si può fare una copia di un programma che si ha in licenza?

Si ma senza commercializzarlo e per l'uso del programma stesso.

Le regole di comportamento previste nella piattaforma di un social network?

Sono regole contrattuali.

Quando sono protette le banche dati?

Sempre se sono rese pubbliche.

Cosa si intende per deterritorializzazione?

La perdita di sovranità derivante dalla tecnologia informatica.

Un nome di dominio è un bene?

Si.

Cos'è la moneta elettronica?

Un valore monetario memorizzato elettronicamente.