Juridical Issues in Computer Science

1 Norme.

Il diritto non può essere normato secondo schemi logici perché i consociati hanno il diritto di conoscere le norme: è necessario un linguaggio parlato e non formale. Un linguaggio parlato è *polisemico*, *ambiguo* e *vago*, per cui il legislatore tenta di aumentare la chiarezza attribuendo nuovi significati a parole già esistenti; mentre l'uso di standard scritti evita la perdita di informazione (rumore) nella trasmissione. Si definiscono più strati di norme:

- Regole tecniche: Sono lo strato più basso delle regole, sono alla pari delle leggi fisiche, non possono essere mutate e non dipendono dalla legislazione vigente.
- Standard (o *soft-law*): Sono basate sulle regole tecniche e la comunità suggerisce il modo considerato migliore per una certa pratica(regole) (standard ISO per l'Europa).
- Norme sociali: sono comportamenti diffusi in una data cultura; sono difficili da modificare anche quando vanno in contrasto con norme positive, riguardano l'uso che facciamo delle regole tecniche.
- Norme positive: Sono lo strato più alto. La parola postive deriva dal latino e significa poste, sono le regole poste dal legislatore; possono anche essere in contrasto con le regole tecniche.

Il diritto è l'interazione tra i vari livelli di regole.
È proprio a causa delle norme sociali che il legislatore non legifera su tecnologie *distruptive*: non essendo noto l'uso, non sono poste regole nell'uso.

Si preferisce utilizzare regolamenti anzichè norme, per le questioni tecniche, per facilitare eventuali modifiche e rendere indipendente la questione da questioni politiche, poiché i regolamenti non devono essere approvati dal parlamento.

2 Obsolescenza.

L'obsolescenza digitale può avvenire per obsolescenza del supporto (dovuta a guasti meccanici o al tempo) o per obsolescenza software (il software utilizzato non è più supportato). Software *open source* e l'uso di formati liberi possono aumentare la longevità dell'informazione.

3 Licenze free.

Le licenze *free* specificano solamente cosa non è permesso fare col software: qualsiasi altra azione è lecita. Il termine *free* non si riferisce appunto al prezzo ma al concetto di libertà: l'utente ha accesso a ogni parte del prodotto, è libero di modificarlo e di redistribuire il prodotto modificato (non però sotto licenze più restrittive). Esistono vari tipi di licenze *free* ma non sono per forza compatibili tra di loro.

Il copyright si differenzia dal diritto d'autore: il primo protegge l'editore garantendo protezione per gli investimenti effettuati, il secondo protegge l'autore garantendogli il controllo dell'opera anche dopo la pubblicazione. Il diritto d'autore moderno si differenzia in diritti morali (inalienabili), che corrispondono all'idea originale del diritto d'autore, e in diritti materiali, che normano come l'opera è accessibile al pubblico (o come sono gestite le opere derivate) che si sovrapone con l'idea del Copyright.

3.1 Storia del *copyright*.

Prima della stampa (prima metà del XVI secolo), un testo scritto era considerato di pubblico dominio; ma con le prime pubblicazioni il sapere si trasmette pressochè invariato nel tempo (senza il *rumore* della forma orale). Il concetto di cultura è cambiato con l'invenzione del libro: indipendentemente dal messaggio contenuto, il sapere è molto più diffuso rendendo difficile dalle autorità controllare le opere

prodotte ed è possibile fare più copie di un libro evitando spostamenti per consultarli. Un autore diffondeva il proprio manoscritto a più stampatori per permettere una maggior diffusione dell'opera; ma nel 1709 l'Inghilterra emana il primo editto sul *copyright* garantendo allo stampatore l'esclusiva: dato l'elevato costo delle apparecchiature, era così riconosciuto all'editore il diritto di proteggere il proprio investimento.

Successivamente, il diritto d'autore nasce con Kant: dopo la pubblicazione di *Critica della Ragion Pura*, circolavano copie modificate da terzi spacciate per originali. Il diritto d'autore è inalienabile e garantisce la paternità dell'opera mentre i diritti materiali normano lo sfruttamento dell'opera.
Precedentemente, gli artisti vivevano sotto la protezione di un Mecenate; ma grazie a questa istituzione un artista poteva vivere delle sue opere, rispondendo univamente al pubblico: i primi furono Beethoven e Manzoni. Il diritto d'autore era stato pensato per durare vita natural durante dell'autore e per i successivi 50 anni (70 nel caso di persone giuridiche) ma, negli anni '80 è stato aumentato di 20 anni (25 nel caso di persone giuridiche) a causa di pressioni della Walt Disney per proteggere il prodotto di Topolino.

Col tempo l'intermediario acquista potere (la distribuzione costa più della metà delle spese complessive), ma l'avvento di Internet modifica leggermente le cose: da una parte i *blog* risparmiano agli autori l'uso del linguaggio HTML per pubblicare, dall'altra nascono nuovi intermediari digitali, non regolamentati. Umberto Eco afferma che con l'avvento di Internet il sapere si appiattisce: è trasmesso tutto allo stesso modo, mentre prima erano selezionati solamente i testi considerati degni di nota dai sapienti del periodo.

3.2 Storia delle licenze software.

Negli anni '60, IBM iniziava a vendere i suoi sistemi UNIX indipendenti dall'hardware: è il primo caso di commercializzazione del software. Tuttavia nell'ambito di ricerca il software è considerato bene comune e viene scambiato gratuitamente senza conseguenze legali: non si applica l'idea di furto perchè non è rimossa la copia originale ma solamente copiata.

Nel 1978, Bill Gates chiede che gli sviluppatori fossero tutelati ricevendo pagamenti a seguito della vendita del software prodotto. Nello stesso anno, negli USA si norma la diffusione del software che segue la medesima fattispecie della musica (ormai in musicassette). Sempre in quegli anni, Bill Gates firma un contratto con IBM per l'installazione di DOS sui PC; successivamente IBM, per rimediare a tale errore, tenta il lancio di OS2, ma senza successo.

Richard Stallman invece teorizza l'informazione libera e le licenze free: chi ha le competenze può modificare un codice sorgente e ridistribuirlo. Nel 1985 fonda la *Free Software Foundation* scrivendo la prima licenza *free* (la GPL[**G**eneral **P**ublic **L**icense]): è esplicitato solamente cosa è vietato. La sua battaglia è una battaglia politica ma mancava un pezzo fondamentale: Il Sistema Operativo che porta avanti il progetto è però sviluppato da Linus Torvalds: egli voleva progettare il miglior sistema operativo esistente, e già le prime versioni di Linux ebbero successo, se pur in una nicchia di esperti, per la stabilità che offriva.

Nel 2002 Edgar David Villanueva Nunez, parlamentare peruviano, propone l'uso di software libero (a parità di qualità) nella digitalizzazione della Pubblica Amministrazione. Microsoft Perù risponde affermando che il costo delle licenze è irrisorio e cita il caso del Messico che aveva informatizzato le scuole messicane con dei computer Linux (quando nessuno aveva le competenze per usarli). Ma l'uso del software libero, afferma Villanueva, è per questioni politiche: è l'unico modo per garantire accesso libero, persistenza dei dati e sicurezza.

La digitalizzazione della Pubblica Amministrazione italiana subisce pressioni da Microsoft Italia che offre licenze gratuite.

3.3 Creative Commons.

L'idea di licenza *open* è stata portata a inizio 2000 al mondo analogico grazie alla licenze *Creative Commons*(CC), che nascono da un idea di Lessig Lawrence un professore di Stanford, pensata per opere artistiche: il concetto di *copyright* è uscito dalla sfera di competenza per cui è stato pensato, rendendo difficile se non impossibile la creazione artistica. Il

termine *Commons* fa riferimento ai beni che, nel diritto anglosassone, non possono essere ridotti a proprietà privata perchè sono di pubblica utilità. Ma non diventano neanche un public domain infatti io posso recintare le mie opere con diverse modalità di licenze:

1. **Solo attribuzione** : Le CC non sono delle public domain e inoltre ha come condizione almeno quella di attribuire l'opera all'autore principale nella sua integrità (nella forma originale). In questo caso uno può fare quello che vuole con la mia opera basta che mi attribuisca l'opera.

2. **Attribuzione** opere **non derivate** : Posso scegliere che non possano esistere delle opere derivate dalle mie senza il mio permesso, in tal caso uno come Mondadori può stampare la mia opera nella sua integrità, attribuendola a me e non mi deve dare i soldi (può convenire se sono un artista alle prime armi o se sono uno scienziato o un accademico come Kant).

3. **Attribuzione** opere **non derivate non commerciali** : Posso aggiungere anche la non commerciabilità, in questo caso tu puoi pubblicarla ma non puoi far pagare il libro senza il mio consenso (possiamo decidere insieme il prezzo ma non lui da solo).

4. **Attribuzione non commerciale** : Permetto tutte le modifiche e derivazioni affinché tu non la vendi. Se la vendi devi prendere il mio permesso.

5. **Attribuzione non commericale condividi allo stesso modo** : Permetto la modifica e la sua divulgazione ma devi ridistribuirla con la stessa licenza con la quale l'ho dato a te e per modificare la licenza devi prendere permesso da me.

6. **Attribuzione non commericale condividi allo stesso modo** : Permetto la modifica e la sua divulgazione ma devi ridistribuirla con la stessa licenza con la quale l'ho dato a te e per modificare la licenza devi prendere permesso da me.

7. **Attribuzione condividi allo stesso modo** : Semplicemente non posso chiudere l'opera che sto mandando in giro, non posso recintarla in nessun modo, l'unica cosa che è che deve essere distribuito allo stesso modo in cui te l'ho diffusa io. In senso tutti gli altri possono prendere l'opera derivata e venderla se l'ho permesso io nell'opera originaria.

3.4 Open Access.

Il MIT, pagando abbonamenti a riviste scientifiche su cui pubblicavano i risultati delle proprie ricerche, presenta il concetto di Open Access: i risultati ottenuti da ricerche finanziate da denaro pubblico devono essere di pubblico dominio. In questo modo i risultati di una ricerca sono fruibili da tutti.

4 Pubblica Amministrazione.

Un documento informatico è facilmente modificabile; dunque per garantire l'inviolabilità è utilizzato il sistema della *firma digitale*, basato su un hash del documento crittografato in modo asimmetrico (la chiave pubblica è quella di decriptazione). Il formato prediletto dalla Pubblica Amministrazione è il PDF/A, che a differenza del PDF standard non permette alcune operazioni sfruttabili da malintenzionati, ad esempio, non permettendo l'inserimento di caratteri nascosti e gif. Inoltre il formato PDF garantisce l'indipendenza del documento dalla stampante in uso (cosa non verificata per i formati DOC e ODT); inoltre è aperto ma non modificabile.

4.1 CAD.

Il *Codice di Amministrazione Digitale*, entrato in vigore all'inizio del 2005, stabilisce una serie di norme per la digitalizzazione della Pubblica Amministrazione. Stabilisce i diritti dei cittadini nei confronti della pubblica amministrazione digitale; per farlo include la definizione di *documento informatico*: questo non può essere modificato (o perlomeno deve essere possibile risalire al modificante). La paternità delle modifiche ad un documento digitale è facilmente attribuibile grazie alla *firma digitale*.

Il CAD definisce anche cosa si intende per *duplicato informatico* (copia digitale di documento digitale) o di *copia informatica di documento analogico*

(documento digitale avente lo stesso contenuto di un documento cartaceo).

4.2 PCT.

Il *Processo Civile Telematico* prevede che in tutti i processi di diritto civile lo scambio di documenti tra le parti avvenga in modo digitale (per ridurre il tempo di trasporto dei documenti cartacei).

4.3 SPID.

Il *Sistema Pubblico di Identità Digitale* è un progetto in tre fasi che sfrutta la firma elettronica per interagire con la Pubblica Amministrazione. Il progetto è diviso in tre fasi:

- Una prima fase in cui l'utente accede a servizi online con credenziali arbitrarie;
- Una seconda fase in cui l'utente accede a servizi con credenziali arbitrarie e un codice temporaneo di accesso;
- Una terza fase in cui l'utente dispone, oltre delle sue credenziali, di un supporto fisico per l'identificazione.

4.4 PEC.

La *Posta Elettronica Certificata*, modellata sulla raccomandata analogica, garantisce l'identità della persona con cui si comunica e permette quindi l'interazione con la Pubblica Amministrazione: è considerato il *domicilio digitale* della persona, anche per quanto riguarda violazione (rientra nella fattispecie delle violazioni di domicilio). Quando una e-mail è inviata da una PEC a un'altra, l'SMTP server invia una conferma di ricezione e registra in automatico il log, sottoscritto da firma digitale, per inviarlo al mittente (senza passare dal destinatario, che quindi non può apportare modifiche). La differenza, rispetto alla raccomandata, è che non è necessario il recepimento di una persona: si ha presunzione di conoscenza nel momento in cui l'email arriva nella casella di posta del destinatario.

5 Sicurezza informatica.

Nel 1984 si è inserita la prima *backdoor* in un compilatore: questo compilava programmi inserendo altre backdoor; successivamente, nel 1995, è stata inserita una backdoor nel compilatore del compilatore: non si può più avere la garanzia che il proprio compilatore sia sicuro. Da questo momento non è più possibile garantire la sicurezza informatica.

A inizio 2000 però si scropre che la maggior parte delle falle di sistema è dovuta ad errori umani: Mitmick (il primo *cybercriminale*) afferma che spesso l'hacking è fatto non con competenze informatiche ma sfruttando il modo con cui gli utenti si interfacciano ad un sistema informatico (ingegneria sociale). Esempio è il *phishing*, ovvero la truffa tramite e-mail (si parla di *spiral-phishing* se mirato verso una data persona).

5.1 Tipologie di attaccante.

Fino al 2000 circa, i virus non avevano scopi malevoli ma servivano solamente per prendere in giro la vittima in contesti amichevoli; col tempo si sono individuate varie tipologie di *hackers*, in base alle modalità e alle finalità dei loro attacchi.

Script-kid. Sono attaccanti senza scopo apparente, spesso con limitate capacità tecniche ma che usano strumenti già implementati.

Attaccanti politici. Spesso gli attaccanti politici (come il movimento *Anonymous*) non hanno grandi capacità tecniche ma sfruttano campagne di marketing per migliorare la propria immagine; se spinti da intenzioni malvage sono definiti anche *cyber-terroristi*.

Industria del malware. Esistono società altamente specializzate il cui oggetto sociale è la produzione di software malevolo su commissione. Esempio è la BSA (Business Software Association), società russa opearativa nel biennio 2007-2008 e sparita senza lasciare tracce.

Squoters. Il loro unico obiettivo è fare danno; generalmente sono dotati di forti capacità tecniche.

Insiders. Sono lavoratori poco soddisfatti della propria condizione che provocano danni alla società o comunicano all'esterno informazioni riservate; è impossibile difendersi.

Hackers etici. Eseguono *pentesting* (anche non autorizzato) e comunicano a chi di dovere le falle di sicurezza trovate nel sistema; generalmente sono dotati di forti capacità tecniche.

5.2 Firma elettronica.

Negli anni '90 i processori sono sufficientemente potenti per implementare algoritmi di crittografia asimmetrica (PGP[**P**retty **G**ood **P**rivacy]): la sicurezza non è data dalla segretezza dell'algoritmo, che è pubblico, ma dalla lunghezza e bontà della chiave. È così rispettata la triade CIA:

- confidenzialità: le informazioni sono leggibili solamente da chi autorizzato;
- integrità: non è possibile modificare i dati senza autorizzazione, e in ogni caso è tenuta traccia delle modifiche;
- accessibilità: se autorizzati, è facile l'accesso ai dati.

È così permessa una sicurezza di tipo militare per il singolo cittadino. L'algoritmo (RSM) è composto da una chiave privata, di decriptazione, e una pubblica, di cifratura: il documento è cifrato con la chiave pubblica del destinatario e inviato a questo che è l'unico in grado di leggere il file.

La Pubblica Amministrazione identifica più livelli di firma digitale:

- FE (Firma Elettronica): dati in forma elettronica acclusi o connessi logicamente ad altri dati elettronici per firmare il documento.
- FEA (Firma Elettronica Avanzata): è connessa unicamente al firmatario ed è idonea ad identificarlo per ogni modifica effettuata nel documento;
- FEQ (Firma Elettronica Qualificata): emessa su un dispositivo qualificato da Ente terzo certificato dallo Stato, ha lo stesso valore di una firma autografa.

Per garantire ulteriormente l'inviolabilità del file, un documento informatico della Pubblica Amministrazione contiene in calce l'hash del documento stesso (in due variazioni diverse), che è l'unica parte crittografata.

Una firma elettronica per poter essere considerata valida deve avere determinate caratteristiche:

- atenticità: la firma deve assicurare il destinatario della libera sottoscrizione del mittente;
- non falsificabilità: la firma deve garantire la provenienza del documento in modo univoco;
- non riusabilità: la firma non deve poter essere usata su altri documenti (garantito dall'algoritmo di hash);
- non alterabilità: un documento firmato non può più essere alterato;
- non contestabilità: il firmatario non può rinnegare la paternità della propria firma.

5.3 NIS.

La direttiva NIS, enrtata in vigore a Novembre 2018, regola il comportamento in caso di attacco a infrastrutture critiche. La ratio è di evitare il ripetersi degli attacchi informatici che hanno colpito l'Estonia, facilitando anche opearzioni tra più Stati, creando un database centralizzato di attacchi informatici, popolato imponendo l'obbligo di segnalazione a determinati centri di interesse (CSTRI) che supportino l'attaccato.

La direttiva si applica ai fornitori di servizi essenziali (individuati dal Ministero dello Sviluppo Economico entro il 9/11/2018) per cui la fornitura del servizio necessita di un Sistema Informativo, e dunque eventuali danni provocano interruzioni della fornitura o danneggiamenti dell'utenza. Inoltre, la direttiva si applica in automatico a fornitori nazionali o con rappresentante nazionale di servizi di *e-commerce*, *search engine* e *cloud*. Sono escluse le PMI (Piccole e Medie Imprese, cioè aziende con meno di 50 dipendenti o meno di 10mln di fatturato annuo).

La direttiva prevede obbligo di segnalazione e di implementare misure tecniche e organizzative di sicurezza proporzionali e adeguate. Inoltre la

direttiva impone la continuazione del servizio anche in caso di attacco informatico. L'obbligo di notifica si applica solamente in caso di incidenti a impatto rilevante:

- sospensione del servizio per 5 milioni ore utente;
- danni a persone tali da compromettere la vita;
- danni per un valore economico pari a €1.000.000 per un cittadino comunitario;
- compromissione dei dati di 100.000 utenti.

La notifica deve avvenire senza giustificato ritardo, con pena pari compresa tra €12.000 e €120.000, comunque contenuta rispetto a quella per la subita violazione di dati personali per insufficiente protezione. La notifica deve comprendere inoltre le policy aziendali di sicurezza e la certificazione di autitor esterni sull'implementazione di tali misure .

6 GDPR.

Secondo la nuova normativa, i dati sensibili tenuti da un'azienda devono essere crittografati (per garantire sia protezione che veridicità).

La regolamentazione della tecnologia, partendo da alcune assunzione di base, la tecnologia è qualunque cosa che si pone come un medium tra l'ambiente e il soggetto che si relazione con tale ambiente. A partire da determinate innovazioni tecnologiche si è sviluppata l'esigenza di tutelare la sfera di riservatezza che è la classica definizione di privacy. A fronte delle PIT (Privacy Invading Technologies) si è creata l'esigenza di tutela e regolamentazione della privacy, ma la risposta non è sempre stata una risposta sempre normativa infatti ci sono le cosiddette PET (Privacy Enhancing Technologies) delle tecnologie che consentivano di rispondere a queste esigenze di tutela con altri strumenti tecnologiche ad esempio la crittografia, anonimato ecc. Anzi spesso è questa risposta non legale ad essere più efficace dei metodi legali con magari delle sanzioni. Ormai la distinzione tra ambiente vs digitale e online vs offline non ha più senso visto l'ambiente in cui ci troviamo.
Se trattiamo la privacy come concetto analogico e non digitale (cioè la privacy non è solo 1 o 0 ma ha dei strati intermedi) quindi ha senso parlare di strumenti che ci permettono di aumentare il livello di protezione dei nostri dati. Il concetto classico della privacy fisica (tutela dall'essere visti in certe circostanze), ovviamente in un contesto digitale è quello della informational privacy, visto che le leggi trattano come privacy le sue informazioni.
Le fasi del ciclo di informazione sono: a) apprensione → b) comunicazione → c) registrazione o archiviazione → d) telecomunicazione (trasmissione) → e) manipolazione
Rispetto a questi step ci sono stati vari sviluppi di tutela, ad esempio dall'ultima fase della manipolazione è nata la data protection. Nel 1890 il primo step in un articolo di Warren e Brandeis in cui si parla del diritto alla privacy, dice che non si possono diffondere le foto senza il consenso dell'individuo, era dovuto alla nascita delle telecamere portatili e della giornale scandalistica, che è uno dei primi oggetti che ha fatto sorgere l'esigenza della privacy.
Un altro step importante nel 1928 con il tema dell'intercettazione delle conversazione dentro le case, la polizia usa strumenti per captare le informazioni (conversazioni) dentro casa di uno spacciatore (il signor Olmstead) senza chiedere autorizzazione del magistratura (è una forma di trespassing ma allora non c'era nessuna legge a riguardo). La corte Suprema da ragione alla polizia poiché non erano mai entrati dentro la proprietà privata quindi nessuna violazione della privacy fisica (ATTENZIONE non c'era ancora informational privacy). L'avvocato Brandeis firma un dissenso dicendo non era d'accordo con il fatto di aver dato ragione alla polizia, dicendo che la legge non era formata in base alla tecnologie che avevano in quel momento altrimenti vi sarebbe stato una legge che avrebbe richiesto il permesso del magistrato per proteggere la privacy del cittadino americano.
Nel 1970 la privacy nel senso tradizionale piano piano si sviluppa a partire da USA, nel 1970 vediamo a livello mondiale la prima forma di regolamentazione dei dati personali, qua la PIT è il computer mainframe. Il problema è dovuto al fatto che non ci si fida ancora del governo tedesco e svedese (per la WWII) e quindi c'è la necessita di regolamentare i dati personali dovute ai censimenti per l'uso che ne potrebbe fare il governo. Le esigenze sono in pratica 2:

- Impedire la nascita di banche dati segrete,

rendere informazione per far sapere al soggetto a cui i dati si riferiscono il perché, la durata del trattamento dei dati.

- Impedire usi secondari di questi dati, se raccogli i dati per un motivo non devi usare i dati per altre finalità.

Queste due esigenze anche oggi sono alla base della data protection. Oggi il caso più famoso della concretizzazione di questi due problemi è quello di Cambridge Analitica.
Differenze nella privacy nel senso tradizionale e data protection:

- • Privacy: Individuo non deve essere sottoposto a ingerenze da parte del pubblico, la sfera ecc. Privacy nel senso tradizionale: Sottrazione del individuo rispetto al contesto.

- Data Protection: Rapporto di fiducia tra uno che gestisce un database (data collector) e l'individuo (data subject) a cui le informazioni si riferiscono, se nella privacy parlavamo della sottrazione qua si parla della limitazioni dell'uso dei dati, può essere definita come una sorte di attrito nella circolazione delle informazione. La privacy (informational) è una sorte di controllo in questo ambito, in particolare la privacy viene definita come la possibilità di decidere in maniera autonoma quando, come e in che misura comunicare ad altri informazione che li riguardano.

L'ultimo step è nel 1994, La copertina di Time dedica la copertina ad internet, la data protection resta un questione legata a data controller e data subject. Qua la banca dati non è più in mano al governo come nel 1970 ma ad internet, quindi il fenomeno di violazione dei dati possono diventare un fenomeno di massa e gli attori principali sono le corporation private.
Nel GDPR la norma che riguarda la sicurezza informatica (Art. 32) ha come primo riferimento, quindi come primo strumento di tutela che il titolare del trattamento (il data controller) deve implementare, quello di incrementare strumenti volti all'anonimizzazione (pseudonimizzazione) e cifratura dei dati personali. Con il GDPR si eliminano le misure minime di sicurezza, essendo un elenco specifico a cui era collegato la sanzione penale dovevano essere tassative, ma con il periodo dovrebbero essere modificate, e per una norma a lunga durata diventerebbero obsolescenti e insicure. E' rimasto il fatto di avere le misure di sicurezza idonee ed adeguate, che sono state specificati almeno 4 ambiti (tra cui anche quello di cifratura dei dati), che rappresentano punti di riferimento che il titolare del trattamento deve tenere in considerazione. I 4 ambiti sono:

1. Cifratura dei dati

2. Utilizzo di sistemi di sicurezza perimetrale quindi avere l'antivirus aggiornato ecc.

3. Procedura Specifica in maniera informatica per garantire in tempi certi la disponibilità e l'accessibilità dei dati.

4. La verifica dei test (penetration test) a cadenza regolari per valutare il livello di sicurezza della propria azienda, per garantire i 3 punti appena elencati.

Elemento fondamentale di questa norma è che tutti i soggetti bene e servizi ai cittadini europei sono tenuti a rispettare il GDPR. Il GDPR tiene in mente i grandi colossi come Facebook, Google ecc. Il nuovo regolamento si basa sull'accountability, fondamentalmente responsabilizzazione e rendicontazione, al data controller sono imposti tutta una serie di oneri che sostituiscono autorizzazioni, in buona sostanza deve predisporre un documento che dovrà descrivere in particolare il tipo di trattamento e dovrà descrivere le misure di sicurezza che ha adottato per limitare il rischio di violazione dei dati personali. Questo documento sarà la policy per tale tipo di trattamento. Il momento in cui si dovesse verificare un problema. In questa normativa viene fornita una cornice che verrà dopo riempita dalle regole tecniche, best practice e formazione specifica da parte dei operatori in modo tale da avere come rifermento con la norma ma patrimonio di conoscenze di un particolare settore. Il 3^o aspetto da considerare è quello di sanzioni, le sanzioni previste sono due tipologie di sanzioni amministrazione con un massimale di 20 milioni per una categoria e 10 milioni per un'altra categoria di violazioni, nelle quali se 20 milioni di

euro dovessero essere considerati poco si può arrivare al 4% del fatturato annuo dell'anno precedente.
Il GDPR è applicabile dal 25 maggio 2018, prima di questa data tutti gli stati membri hanno avuto 2 anni dal maggio 2016 per emanare delle norme di coordinamento con la norma nazionale e quella europea. In Italia il d.lgs. 101/2018 (per il coordinamento) è entrato in vigore il 19 settembre 2018. I 6 punti fondamentali della data protection sono:

1. Fondamenti di liceità del trattamento: Ogni trattamento del dato personale che non sia svolto per motivi personali, deve basarsi su un fondamento di liceità (e quindi avere una base giuridica).

2. Informativa: I contenuti dell'informativa sono elencati in modo tassativo nel regolamento e in parte sono più ampi rispetto al Codice. Nell'informativa ci dovrà essere il titolare del trattamento, la finalità del trattamento e la base giuridica del trattamento.

3. Diritti degli interessati: Il titolare deve dare entro 1 mese dalla richiesta una risposta all'interessato e i diritti sono:

    - Diritto di accesso
    - Diritto di rettifica
    - Diritto di cancellazione (nuovo)
    - Diritto di limitazione
    - Diritto alla portabilità (nuovo)
    - Diritto di opposizione
    - Diritto di revocare il consenso

4. Titolare, responsabile e incaricato

5. Approccio basato sul rischio e misure di accountability

6. Trasferimenti di dati verso paesi terzi

La normativa, che in generale si applica solo alle persone fisiche (l'interessato), per quanto riguarda l'attività promozionale sia applica sia alle persone fisiche che alle persone giuridiche. Un dato non deve essere considerato pubblico solo se facilmente reperibile su internet. Un dato è pubblico se viene da determinate tipi di fonti che lo codificano come tale. Potrebbe essere che uno li abbia pubblicati per un altro motivo e io non posso cambiarne la finalità solo perché disponibile online. Questa sorta di raccolta dei dati ad esempio per arricchire i database è vietata dalla normativa europea e italiana. La normativa del 2013 individua una serie di modalità volta alle attività promozionale rispetto a queste modalità stabilisce e sceglie se esiste un obbligo di consenso preventivo (opt-in) o il di consenso preventivo – eccezione (opt-out) (posso oppormi al trattamento) Gli aspetti dell'attività promozionale sono due:

- L'informativa che specifica non solo l'attività promozionale ma anche la modalità di come questa attività promozionale viene raggiunta, quindi se ti contattano tramite il telefono, mail ecc.

- Rispetto a tale modalità ricevere il consenso se necessario dell'interessato. Il consenso è la seconda modalità, in questi casi parla di opt-in.

Quindi non mi è consentito mandare le mail esplorative per richiedere il consenso se non l'ho a monte. Ma è possibile contattare telefonicamente mediante un operatore fisico per ricevere il consenso del contraente per ricevere comunicazione promozionale, ma si ha la possibilità di disiscriversi (opt-out) ad esempio iscrivendosi al registro delle opposizioni, un altro ambito dvoe si può esercitare il diritto all'opt-out è quello di marketing postale.
Il consenso deve essere staccato rispetto all'erogazione del servizio, rispetto alla raccolta di altri dati, deve essere libero e si deve basare sull'informativa. Queste caratteristiche sono rimaste anche nel GDPR.
Oltre al opt-in, opt-out esiste un terzo regime soft-spam in cui trattiamo i dati del nostro cliente, il cliente nel contratto ci lascia l'email o indirizzo postale, e prevede la possibilità di usare email o indirizzo per inviare comunicazioni di tipo promozionale o commerciale.
Per i dati sanitari invece, prima del GDPR c'era il divieto di utilizzare i dati sanitari salvo un autorizzazione del Garante, un informativa, consenso scritto e consenso scritto al trasferimento verso paesi terzi (in caso ce ne fosse bisogno). Il GDPR ha ribadito il fatto che il dato non è utilizzabile

se non da un autorizzazione dell'interessato e non fosse per un uso pubblico, non è possibile farne uso promozionale, di profilazione o qualunque non consentito dall'utente. I dati della regione Lombardia potevano essere usati dopo l'anonimizzazione da un operatore. Le norme di sicurezza sono delle norme specifiche, devono garantire la segregazione dei dati, garantire i vari livelli di accessibilità dei dati in modo che non tutti possano accedere a tali dati e garantire la cifrature e copertura dei dati e garantire la data-recovery e comunicazione dei breech che hanno ricevuto.
La privacy su internet, l'elemento fondamentale è il cookie, i cookie sono divisibili in due macro categorie: cookie di prima parte (di tipo tecnico) e di terza parte (di profilazioni). Il 99% dei cokie utilizzati sono di terza parte. In mezzo ai due tipi di cookie c'è un terzo tipo quello di cookie analitici che permettono di vedere le statistiche riguardante le pagine, e questi possono essere usati senza adempiere una serie di obblighi solo se sono anonimizzati. Per l'uso dei servizi cloud regole particolari non ne sono state introdotte, sta al cliente di scegliere il cloud che possa fornire un certo livello di sicurezza.

6.1 *Cyber Act.*

L'Organo Europeo ENISA, entro fine anno, stabilirà una bozza di regolamento (quindi valido senza recepimento da parte dei Paesi membri) per la certificazione di oggetti IoT e simili.