



DIRITTO DELL'INFORMATICA E DELLE COMUNICAZIONI

Appunti Lezioni – Anno 2020/2021



GAIA SERAVELLI

Sommario

Diritto dell'Informatica (Informatica Forense)	22.02.21	5
Differenza tra Diritto Civile e Penale.....		6
Art. 24 Costituzione:.....		6
Art. 63 Dichiarazioni Indizianti:.....		6
Procedimento Civile.....		7
Prove		7
Consulente Tecnico		7
Procedimento Penale		8
1. Fase di Indagine.....		8
2. Fase Processuale		8
Art. 111		8
Prove		8
Art.27 Costituzione:.....		8
Documenti e Firme 04.03.21		10
Art. 2699 Atto Pubblico:.....		10
Art. 2702 Scrittura Privata:		10
Art. 2703 Sottoscrizione Autenticata:.....		10
Da Art.22 a 23 Copie Informatiche. -Codice Amministrazione Digitale.....		10
Art. 24 Firma Digitale. -Codice Amministrazione Digitale.....		11
Regolamento Europeo 08.03.21.....		12
Cap. 8, paragrafo 1.....		12
Cap. 8, paragrafo 2		12
Cap. 8, paragrafo 4		12
CAPO I		12
Art. 1 Perimetro di Applicazione del Regolamento:.....		12
Art. 2 Ambito di Applicazione Materiale:.....		13
Art. 3 Ambito di Applicazione Territoriale:.....		13
Art. 4 Definizioni		13
CAPO II		14
Art. 5 Principi Applicabili al trattamento di dati personali (Cuore del regolamento Europeo)		14
11.03.21		15
Art. 6 Liceità del trattamento (quando un trattamento è lecito)		15
Art. 9 Trattamento di categorie particolari di dati personali.....		15
Art. 10 Trattamento dei dati personali relativi a condanne penali e reati.....		17
Art. 7 Condizioni per il consenso		17
Art. 8 Condizioni applicabili al consenso dei minori in relazione ai servizi della società dell'informazione		18
Art. 11 Trattamento che non richiede l'identificazione.....		18
CAPO III (L'Informativa)		18

Art. 12	18
Art. 13 Informazioni da fornire qualora i dati personali siano raccolti presso l'interessato	18
Art. 14 Informazioni da fornire qualora i dati personali non siano raccolti presso l'interessato	19
Diritti degli Interessati	19
Art. 15 Diritto di accesso dell'interessato	19
Art. 16 Diritto di Rettifica	19
Art. 17 Diritto alla Cancellazione (diritto all'Oblio)	19
Art. 18 Diritto di limitazione di trattamento	20
Art. 19 Obbligo di notifica in caso di rettifica o cancellazione dei dati personali o limitazione del trattamento	20
Art. 20 Diritto alla portabilità dei dati	20
Art. 21 Diritto di opposizione	20
Art. 22 Processo decisionale automatizzato relativo alle persone fisiche, compresa la profilazione	20
Art. 23 Limitazioni	20
15.03.21	20
CAPO IV (Titolare del trattamento e responsabile del trattamento)	20
Art. 24 Responsabilità del Titolare del Trattamento (Data Controller/Owner)	20
Art. 25 Protezione dei dati fin dalla progettazione e protezione dei dati per impostazione predefinita	21
Art. 26 Contitolari del Trattamento	21
Art. 28 Responsabile del Trattamento (Data Processor)	21
Art. 29 Trattamento sotto l'autorità del titolare del trattamento o del responsabile del trattamento	22
Art. 30 Registro dei Trattamenti	22
Art. 32 Sicurezza del Trattamento	22
Art. 33 Notifica di una violazione dei dati personali all'autorità di controllo	22
18.03.21	23
Art. 37 Designazione del responsabile della protezione dei dati (Data Protection Officer DPO)	23
Art. 38 Posizione del responsabile della protezione dei dati	23
Art. 39 Compiti del responsabile della protezione dei dati	24
CAPO V	24
Art. 44 Principio generale per il trasferimento dei dati all'estero	24
Art. 45 Trasferimento sulla base di una decisione di adeguatezza	24
Art. 46 Trasferimento soggetto a garanzie adeguate	24
Art. 47 Norme vincolanti d'impresa	24
CAPO VIII	25
Art. 83 Condizioni generali per infliggere sanzioni amministrative pecuniarie	25
Classificazione dei soggetti	25
Dark Web 22.03.21	26
25.03.21	27
Servizi Dark Web	27

Decloaking	28
Bitcoin 01.04.21.....	28
Altre Criptovalute.....	30
08.04.21	31
Smart Contract 03.05.21	31
Reati Informatici 29.04.21.....	34
Riservatezza delle Informazioni	34
Art. 616 -Codice Penale.....	35
Art. 15 -Costituzione	35
Art. 617 e 617bis -Codice Penale	35
Art. 617-ter -Codice Penale.....	35
Art. 617-quater, Art. 617-quinquies, Art. 617-sexies -Codice Penale	35
Art. 617-septies Diffusione di riprese e registrazioni fraudolente	36
Art. 618 Rivelazione del contenuto di corrispondenza.....	36
Reati contro il Patrimonio.....	36
Art. 615-quater Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici.....	36
Art. 615-quinquies Diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico	36
Art. 635 Danneggiamento	37
Art. 635-bis Danneggiamento di informazioni, dati e programmi informatici	37
Art. 635-ter Danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità	37
Art. 635-quater Danneggiamento di sistemi informatici o telematici.....	37
Art. 635-quinquies Danneggiamento di sistemi informatici o telematici di pubblica utilità	37
05.05.21	38
Reati contro la Persona	38
Delitti contro la vita e l'incolumità individuale	38
Art. 575 Omicidio	38
Art. 595 Diffamazione	38
Art. 599 Provocazione	38
Dei delitti contro la libertà individuale	38
Art. 600-ter Pornografia minorile	38
Art. 600-quater Detenzione di materiale pornografico	39
Art. 600-quater.1 Pornografia virtuale	39
Delitti contro l'egualianza.....	39
Art. 604-bis Propaganda e istigazione a delinquere per motivi di discriminazione razziale etnica e religiosa .	39
Art. 609-bis Violenza sessuale.....	40
Art. 609-quater Atti sessuali con minorenne.....	40
Art. 609-sexies Ignoranza dell'età della persona offesa	40

Art. 609-octies Violenza sessuale di gruppo	40
Art. 609-unidcies Adescamento di minorenni	40
Art. 612-bis Atti persecutori	41
Art. 612-ter Diffusione illecita di immagini o video sessualmente espliciti (Revenge Porn)	41
Come L'informatica impatta sul Diritto	41
Riciclaggio	42
Art. 648 Ricettazione.....	42
Art. 648-bis Riciclaggio.....	42
Computer Forensics (opzionale per l'esame, non la chiede)	43
Art. 359 Accertamenti Tecnici -Codice Penale (ripetibili)	43
Art. 360 Accertamenti Tecnici Irripetibili -Codice Penale	43
Sequestro Probatorio	43
10.05.21	44
Attori dei Crimini Informatici.....	44
Scene del Crimine	45
Reati.....	45
Time Line di un'Indagine.....	45
Modalità d'Indagine (Raccolta delle fonti di prova)	45
Strumenti del Mestiere.....	45
Reati.....	46
Art. 640 Truffa (normale).....	46
Art. 640-ter Frode informatica.....	46
Art. 612-bis Atti Persecutori	46
Art. 494 Sostituzione di Persona.....	46
Indagine su Profili Facebook.....	47

Materia che è legata al mondo del **Diritto** ed è vincolata alle sue convenzioni, ma è anche legata al mondo dell'**Informatica** ed è quindi in continua evoluzione.

Un **Contratto** è qualcosa che regola il rapporto tra due persone, fisiche o giuridiche. Dal momento che io faccio qualcosa per un'altra persona, sto formulando un contratto.

Il contratto:

- È un atto di volontà (accordo tra le parti): devono esserci due volontà che si incontrano.
- Deve avere un oggetto: qualcosa di esistente e possibile (non necessariamente tangibile).
- Deve avere una causa: perché l'ordinamento mi permette di formulare quel contratto. La funzione economica sociale del contratto. (Nella compravendita: lo scambio di un bene con un altro bene)
- Forma: ha una forma libera, quindi se io vendo un bene oralmente è valido. Ciò che io posso fare fisicamente, posso farlo ora anche col mio computer, ed è comunque una forma valida.

La **patologia** del contratto è legata principalmente alle figure di:

- Nullabilità: un contratto nullo è come se non esistesse. Non può essere sanato, ma solo convertito.
- Annullabilità: un contratto annullabile può essere sanato, valido e efficace. La nullità deve essere fatta valere dalla parte che intende eccepirla, entro 5 anni dalla stipula del contratto o dal raggiungimento della maggiore età se la parte era minorenne.

Vizi del contratto (Non li chiede all'esame):

- Errore (visto nella parte degli Smart Contract)
- Violenza: violenza relativa, non assoluta, altrimenti ci sarebbe la nullità del contratto perché non ci sarebbe la volontà. Deve essere determinata da una minaccia concreta di un danno in grado da incutere una paura idonea al soggetto contraente.
- Dolo: tutti quegli artifici e raggiri posti in essere dal contraente per ottenere la stipula del contratto.

L'**Informatica Giuridica** è la materia base del Diritto dell'Informatica, e può essere scomposta in:

Informatica per il giurista

Cioè come l'informatica ha cambiato il mondo del Diritto ed ha aiutato il giurista.

Diritto dell'Informatica

Come il diritto è entrato nel mondo dell'informatica

Entrambe sono indispensabili, e l'una non ha senso senza l'altra. Non possiamo infatti punire un crimine se non è stata preventivamente stabilita una legge che vieti quella specifica condotta (princípio del **Diritto Penale**).

Per parlare di Diritto dell'Informatica bisogna necessariamente avere delle conoscenze informatiche.

La prima domanda che dobbiamo porci quando ci troviamo di fronte ad una prova informatica (documento digitale) è: quanto è attendibile? Quanto è facile e possibile falsificare questo documento?

La risposta è: tantissimo. In informatica, infatti, le cose non sono sempre come sembrano.

Un documento informatico ha una struttura a 3 livelli:

1. Contenitore: il file che contiene l'informazione.
2. L'informazione vera e propria.
3. Meta-informationi: cioè tutte quelle informazioni aggiuntive che io posso ricavare dall'analisi del contenitore.

Ad esempio: avendo una fotografia digitale di un gatto, il contenitore sarà il file jpeg, l'informazione vera e propria sarà l'immagine del gatto, e i metadati saranno l'ora esatta in cui è stata scattata la foto, dove è stata scattata, ecc...

Esiste un rapporto imprescindibile tra il diritto e l'informatica. Devo sapere quindi cosa poter fare giuridicamente e cosa posso fare praticamente. Ad esempio, se devo confiscare una pagina web, devo sapere che giuridicamente posso bloccare la sua homepage, e praticamente posso cristallizzare la directory del sito che si trova nel server.

Queste due cose non sempre coincidono: il fatto che io posso fare qualcosa praticamente, non vuol dire che sia legale dal punto di vista giuridico e, viceversa, se io posso fare qualcosa legalmente, non vuol dire che sia fattibile praticamente.

Gli strumenti cambiano con il tempo, ma non cambia l'uso che ne viene fatto: un contratto scritto con una macchina da scrivere, o con un computer, è la stessa identica cosa.

Ciò sta ad indicare come le cose non siano poi tanto cambiate.

Quello che contraddistingue i sistemi informatici è la possibilità di avere più informazioni in un minor spazio, e quella di comunicare più velocemente. Alla fine dei conti non sono i computer in sé l'innovazione, ma l'uso che ne facciamo.

Licenza informatica: contratto tra noi e chi ha sviluppato il software. Ci consente di usare il sw e di svolgere con esso le attività che vogliamo svolgere.

Differenza tra Diritto Civile e Penale

Non esiste un solo processo, ma tanti. È riduttivo parlare della differenza tra diritto civile e penale, mentre è più corretto parlare della differenza tra procedimento civile e penale.

Processo: accertamento di un giudice relativamente ad un fatto. Ha sempre un inizio e una fine.

Procedimento: sequenza di atti giuridici, posti in essere da uno o più soggetti, tesi ad arrivare ad un atto finale. Da un procedimento possono scaturire anche più processi (1°, 2°, 3° grado, Cassazione...).

I procedimenti civili e penali hanno delle cose in comune: la presenza delle parti, un magistrato e una fine (una sentenza: provvisoria o definitiva).

Art. 24 Costituzione:

"La difesa è un diritto inviolabile in ogni stato e grado del procedimento"

Senza difesa (presenza dell'avvocato) non può esserci il processo.

Art. 63 Dichiarazioni Indizianti:

"Se davanti all'autorità giudiziaria, una persona non imputata (non sottoposta alle indagini) rilascia dichiarazioni che fanno emergere indizi di reità a suo carico, l'autorità ha l'obbligo di interrompere l'esame e avvertire la persona che a seguito di tali dichiarazioni potranno essere svolte indagini nei suoi confronti, e la invita a nominare un difensore."

"Se tale persona, invece, è imputata, le sue dichiarazioni non possono essere utilizzate."

Procedimento Civile

Strumento giuridico con cui si cerca di dirimere le controversie aventi come oggetto questioni di diritto privato, ovvero per questioni che riguardano i privati (persone fisiche, cioè gli umani, sia persone giuridiche, che società, enti, associazioni...).

Può avere varie fasi:

1. Fase **Stragiudiziale**: dove si cerca di arrivare ad un accordo prima del processo, o si contestano determinate condotte.
2. Fase **Giudiziale**: processo vero e proprio.
3. Fase **Esecutiva**: la parte che ha vinto cerca di incomberre sulla parte perdente, la sentenza del giudice.

Ha il principio del petitum (richiesta):

- **Petitum Immediato**: il provvedimento concreto che chiedo al giudice. (es.: chiedo che Tizio restituisca la penna che mi ha rubato)
- **Petitum Mediato**: il diritto che la parte si prefigge di tutelare. (es.: il diritto di Tizio alla proprietà e al possesso della penna)
- **Causa Petendi**: fatti costitutivi del diritto che la parte intende far valere in giudizio. (es.: il contratto di acquisto della penna)

Prove

Una cosa accomuna tutti i processi: il **principio dell'onere della prova**, ovvero chiunque faccia un'affermazione, ha l'onere giuridico di provarne la veridicità.

Le prove sono onere della parte, quindi il giudice non può autonomamente acquisire prove durante il processo civile. Il giudice deve valutare le prove secondo il suo prudente apprezzamento, salvo che la legge disponga altrimenti. Egli può desumere argomenti di prova dalle risposte che le parti gli danno, dal loro rifiuto ingiustificato a consentire le ispezioni che egli ha ordinate e, in generale, dal contegno delle parti stesse nel processo.

Le prove che possono essere usate sono solo quelle previste e disciplinate dal legislatore: documenti, esame testimoniale, ispezioni, accertamenti tecnici.

Esistono prove **costituite**, cioè quelle che pre-esistono al processo, e prove **costituende**, cioè quelle che si formano all'interno del processo.

Prove **dirette**: pongono il giudice a diretta conoscenza del fatto che si vuole dimostrare.

Prove **indirette**: necessitano di un'operazione logica per risalire al fatto da provare.

Prove **piene**: prove assolute, rappresentano il fatto nella sua interezza o in maniera incontrovertibile.

Prove di **verosimiglianza**: si fonda su un criterio di credibilità ed è sufficiente per la concessione di determinati provvedimenti. Prova non piena e assoluta ma convincente.

Argomento di prova: fornisce degli elementi in base ai quali possiamo valutare le prove.

Qui abbiamo due parti, una contro l'altra, con pari poteri.

Consulente Tecnico

È un esperto in un determinato settore, la cui competenza non appartiene al giudice. Il giudice però non è vincolato al Consulente Tecnico, ma può discostarsi dalle sue deduzioni fornendo le opportune motivazioni.

I consulenti tecnici vengono scelti da un albo, ma il giudice può assumere anche un consulente non iscritto all'albo, motivando la sua scelta.

È il giudice che dice cosa fare al tecnico, in base a ciò che vuole sapere.

Il consulente non può rifiutarsi di eseguire l'incarico ma può essere "licenziato" se non è in grado di svolgere il compito.

Procedimento Penale

Molte delle cose del processo civile rimangono invariate.

Tra le cose che variano abbiamo le fasi del procedimento:

1. Fase pre-processuale: indagini preliminari e difensive, effettuate dal Pubblico Ministero (PM).
2. Fase processuale:

- Udienza preliminare: quella che determina il rinvio a giudizio o meno della persona.
- Dibattimento
- Esecuzione: come viene fatta scontare la pena.

1. Fase di Indagine

Si avvia con la comunicazione della **notizia criminis**, oppure con la nomina del difensore, ed è finalizzata a raccogliere gli elementi di prova da utilizzare nelle successive fasi del processo.

Protagonisti di questa fase: **PM e PG** (Polizia Giudiziaria).

Protagonisti accidentali: Difensore, Investigatori e i Consulenti Tecnici, GIP (Giudice per le Indagini Preliminari). (non sono essenziali allo svolgimento del processo)

2. Fase Processuale

Parte con l'**udienza preliminare**, passa alla **scelta del rito** che può essere: abbreviato, applicazione sulla pena su richiesta (Patteggiamento), o Dibattimento. Oppure può esserci un procedimento per **Decreto**.

Art. 111

"Il giusto processo è un principio fondamentale e stabilisce come e quando, un soggetto può essere giustamente condannato."

Prove

Sono oggetto della prova i fatti che si riferiscono all'imputazione, alla punibilità e alla determinazione della pena, e non altri fatti, come ad esempio le abitudini morali dell'imputato o i suoi precedenti giudiziari a meno che non siano rilevanti per il caso. Non si può processare il comportamento della persona ma solo la condotta della persona in quella determinata fattispecie.

La prova è libera, quindi non è ammessa l'ipnosi, la tortura, o droghe per carpire la prova dalla persona.

Quando è richiesta una prova non disciplinata dalla legge, il giudice può assumerla se essa risulta idonea ad assicurare l'accertamento dei fatti e non pregiudica la libertà morale della persona.

Le prove ottenute illegittimamente non sono utilizzabili.

Qui abbiamo lo **stato contro un cittadino**. Quindi il potere dello stato deve essere regolato in modo molto più dettagliato.

Art.27 Costituzione:

"Nessuno può essere ritenuto colpevole fino alla sentenza definitiva, ed è compito dello stato, attraverso un giusto processo, di dimostrare la colpevolezza di una persona."

In questo caso, la prova, rientra nel concetto di **prova scientifica**: deve essere soggetta a contoprova, alla possibilità di essere ripetibile (altrimenti deve essere prima cristallizzata per poter essere riprodotta successivamente), e falsificabile (alterabile, cambiando gli elementi in gioco).

Tipi di documenti:

Art. 2699 Atto Pubblico:

“È il documento redatto, con le richieste formalità, da un notaio o da altro pubblico ufficiale autorizzato ad attribuirgli pubblica fede nel luogo dove l’atto è formato.”

Art. 2702 Scrittura Privata:

“E’ un atto che viene stipulato tra due soggetti, senza particolari formalità. Essa costituisce piena prova, fino a querela di falso, della provenienza delle dichiarazioni da chi l’ha sottoscritta, se colui contro il quale la scrittura è prodotta ne riconosce la sottoscrizione.”

Ad esempio, un'email, se non viene disconosciuta, può essere considerata un documento di scrittura privata. Tuttavia, tutti i supporti che non permettono di riconoscere la grafia del soggetto, rientrano nell'ambito delle riproduzioni meccaniche. Tali riproduzioni hanno stesso valore della scrittura privata, se colui contro il quale la riproduzione è stata prodotta non ne disconosce la conformità ai fatti o alle cose medesime. Quindi se viene presentata una fotografia e io non posso dimostrare che quella fotografia è falsa, essa costituisce una prova di quello che rappresenta.

Art. 2703 Sottoscrizione Autenticata:

“Si ha per riconosciuta, quindi non ho bisogno che l’altra parte la riconosca come propria, la sottoscrizione autenticata da un notaio o altro pubblico ufficiale.”

Tutti questi documenti citati sopra, non comprendono i documenti informatici, né gli strumenti per le comunicazioni a distanza, che sono stati introdotti successivamente dal **Codice delle Comunicazioni Elettroniche** (2003) e il **Codice dell’Amministrazione Digitale**. Quest’ultima, trattando di documenti elettronici, tratta anche delle firme elettroniche e delle modalità della comunicazione a distanza.

Il legislatore ha fatto innanzitutto una distinzione tra **documento digitale e analogico**, dove per documento digitale si intende un documento creato con strumenti elettronici, mentre per analogico un documento creato con strumenti non elettronici.

Il **documento informatico** è un documento elettronico che contiene la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti. Qualsiasi **supporto** può costituire un documento: floppy, hardisk, registrazione audio, muro su cui è tracciata una scritta...

Da Art.22 a 23 Copie Informatiche. -Codice Amministrazione Digitale

Con **copia informatica di documento analogico** si intende un documento informatico che ha contenuto identico a quello del documento analogico da cui è tratto. (es.: faccio una registrazione audio di me che leggo un documento cartaceo. Oppure la scannerizzazione di un documento cartaceo.).

Con **copia analogica di documento informatico** si intende la semplice stampa di un documento digitale.

Con **copia per immagine** su supporto informatico di documento analogico, invece, si intende avere forma e contenuto identici a quello del documento analogico da cui è tratto. Tecnicamente questa è una sciocchezza perché un documento informatico non potrà mai avere stessa forma di un documento analogico. Con questa definizione si volevano identificare le fotografie: se io faccio una foto digitale ad una pagina di un libro avrò una copia informatica di doc. analogico su supporto informatico, se poi faccio

interpretare i simboli della mia foto e creo un PDF leggibile, avrò una copia per immagine su supporto informatico di un doc. analogico.

Copia informatica di documento informatico: non è altro che un copia e incolla del testo di un documento informatico su un altro tipo di documento. Ad esempio, se copio un file word e lo trasformo in PDF, avrò un file identico ma con sequenza di valori binari differente. (I due documenti *non* hanno lo stesso hash) Mentre se faccio una semplice copia, nello stesso formato, avrò due documenti identici tra i quali non potrò distinguere l'originale.

Art. 24 Firma Digitale. -Codice Amministrazione Digitale

La firma elettronica deve riferirsi in maniera univoca ad **un solo soggetto**. Questo non vuol dire ad una sola persona fisica; un'associazione è infatti considerata un **soggetto giuridico**, così come lo è un sindacato, un'azienda, ecc...

Le firme elettroniche sono le più **sicure** in assoluto, decisamente più sicure delle firme autografe. Questo perché posso cambiare la mia firma digitale in qualunque momento e posso avere anche infinite firme digitali per cose diverse.

Firma elettronica: è l'Hash (stringa alfanumerica di lunghezza predefinita). È un algoritmo che viene applicato ad un file e che parte da una sequenza di dati per arrivare ad una sequenza predefinita. È praticamente un riassunto. L'hash è in grado di rilevare anche il più piccolo cambiamento apportato al documento perché, quando ciò avviene, cambia la sequenza di bit; è quindi importantissimo per vedere se un documento ha subito o meno modifiche.

Firma Elettronica Avanzata: è l'insieme di dati in forma elettronica, allegati oppure connessi a un documento informatico, che consentono l'identificazione del firmatario del documento e garantiscono la connessione univoca al firmatario. È un sistema a doppia chiave crittografica.

Firma Elettronica Qualificata: è una firma elettronica avanzata basata sul certificato qualificato. Il soggetto che mi ha dato il dispositivo di firma, lo ha certificato garantendo la mia identità. Se questo sistema di firma elettronica qualificata è basato su un sistema a doppia chiave (pubblica-privata), allora parliamo di Firma Digitale.

Per ottenere una firma elettronica, infatti, un **certificatore** deve riconoscerci in base a: qualcosa che sappiamo (password), o a qualcosa che abbiamo (token), o in base a qualcosa che siamo (dati biometrici).

Il documento informatico è valido (ha stessa validità delle scritture private) se è **regolarmente formato**, cioè quando gli è stata posta una firma elettronica qualificata, una firma digitale o una firma elettronica avanzata.

Il Garante per la protezione dei dati personali è una figura fondamentale prevista dal regolamento e dalla legge d'attuazione del regolamento, con compiti specifici.

Quando si parla di protezione dei dati personali, si tende a parlare di privacy, in realtà questo non è corretto in quanto la privacy è solo un aspetto della protezione dei dati, legato alla loro riservatezza.

La protezione invece è qualcosa che opera a 360°: riservatezza, integrità e disponibilità dei dati (C.I.A.).

Cap. 8, paragrafo 1

"La protezione delle persone fisiche con riguardo al trattamento dei dati di carattere personale è un diritto fondamentale dell'unione Europea."

Quindi il diritto alla riservatezza è un diritto di pari rango al diritto alla salute, alla vita, alla libertà, ecc... È un diritto costituzionalmente garantito.

Cap. 8, paragrafo 2

"I principi e le norme a tutela delle persone fisiche con riguardo al trattamento dei dati personali dovrebbero rispettare i diritti e le liberà fondamentali, in particolare deve prescindere dalla loro nazionalità o dalla loro residenza."

Cap. 8, paragrafo 4

"Il diritto alla protezione dei dati personali non è una prerogativa assoluta, ma va considerato alla luce della sua funzione sociale e va contemporaneo con altri diritti fondamentali."

È un diritto molto importante ma va bilanciato con gli altri diritti dell'unione europea. Nessun diritto è mai assoluto, ma relativo ai diritti delle altre persone.

Indipendentemente da dove sono collocati i server e trattate le notizie, il diritto europeo si applica a tutti i soggetti che trattano dati di cittadini europei o nell'ambito dell'unione europea.

In passato, alcune aziende (come i call center), collocavano la loro attività all'estero e si chiamavano fuori dal Regolamento Europeo. Oggi ciò non è più possibile, perché queste pratiche di elusione non sono più messe in moto.

I nostri dati hanno molto valore, ecco perché devono essere protetti. Con la globalizzazione e l'avanzamento della tecnologia, questo compito è diventato più difficile. Il regolamento europeo non vuole infatti bloccare la circolazione dei dati, bensì vuole che questa circolazione avvenga in maniera corretta, rispettando i diritti dei cittadini.

CAPO I

Art. 1 Perimetro di Applicazione del Regolamento:

1. Il regolamento stabilisce norme relative alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché norme relative alla libera circolazione di tali dati.

2. Il regolamento protegge i diritti e le liberà fondamentali delle persone fisiche, in particolare il diritto alla protezione dei dati personali.

3. La libera circolazione dei dati personali nell'Unione non può essere limitata né vietata per motivi attinenti alla protezione delle persone fisiche con riguardo al trattamento dei dati personali."

Persone fisiche = il regolamento non si applica alle aziende, agli enti giuridici o alle associazioni. Solo alle persone umane. Le aziende hanno diritto ad altre cose (brevetti, segreti industriali), ma non a questa protezione dei dati personali.

Dati personali = non dei brevetti o dei segreti industriali, o altro.

Art. 2 Ambito di Applicazione Materiale:

"Il regolamento si applica a qualsiasi trattamento parzialmente o integralmente automatizzato dei dati personali, e al trattamento non automatizzato."

Ci sono solo poche eccezioni per le quali il regolamento non si applica:

- i trattamenti di dati relativi al contrasto al terrorismo, alla criminalità organizzata, alla diffusione delle pandemie, ecc...
- se i trattamenti sono effettuati da una persona fisica per l'esercizio di attività di carattere esclusivamente personale o domestico. (Es.: io posso scattare una foto di una persona per associarla al suo contatto in rubrica, ma non posso condividerne con nessuno tale foto.)
- se i trattamenti sono effettuati per attività che non rientrano nell'ambito di applicazione del diritto dell'Unione Europea.

Art. 3 Ambito di Applicazione Territoriale:

"Il regolamento si applica al trattamento dei dati personali effettuato nell'ambito delle attività di uno stabilimento da parte di un titolare del trattamento o di un responsabile del trattamento nell'Unione, indipendentemente dal fatto che il trattamento sia effettuato o meno nell'Unione."

Quindi se una persona è stabilita nell'Unione Europea, il regolamento le si applica.

"Il regolamento si applica al trattamento dei dati personali di interessati che si trovano nell'Unione, effettuato da un titolare del trattamento o da un responsabile del trattamento che non è stabilito nell'Unione, quando le attività di trattamento riguardano:

- a) *Offerta di beni o prestazione di servizi a soggetti nell'Unione*
- b) *Monitoraggio del loro comportamento se questo ha luogo all'interno dell'Unione"*

Art. 4 Definizioni

1) **Dato personale:** qualsiasi informazione riguardante una persona fisica identificata o identificabile. Che mi permette quindi di identificare la persona. (anche il numero di scarpe è un dato personale)

2) **Trattamento:** qualsiasi operazione o insieme di operazioni, applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, l'uso, la conservazione, l'adattamento o la modifica, ecc...

3) **Limitazione al trattamento:** il contrassegno dei dati personali conservati come non trattabili, quindi impedisce al titolare del trattamento di trattare questi dati.

4) **Profilazione:** qualsiasi forma di trattamento automatizzato di dati personali, consistente nell'utilizzo di tali dati per valutare determinati aspetti personali relativi ad una persona fisica. È possibile profilare il soggetto, ma questa profilazione deve essere nota al soggetto."

5) **Pseudo anonimizzazione:** i dati vengono trattati in maniera tale da non essere direttamente riconoscibili se non si è in possesso di una chiave di decrittazione. (Es.: pubblicare i risultati degli esami con solo il numero di matricola, quindi un dato non direttamente riconducibile ad un determinato soggetto)

6) **Archivio:** qualsiasi insieme strutturato di dati personali, accessibili secondo criteri determinati, quindi organizzati in maniera tale che io possa ricercare tali dati.

7) **Titolare del trattamento:** il soggetto, che può essere una persona fisica o giuridica, che tratta dati personali, e stabilisce relativamente a questi dati, le finalità e i mezzi del trattamento. È lui che stabilisce quale dati trattare e come trattarli.

8) **Responsabile del trattamento:** soggetto che viene incaricato dal Titolare del trattamento, e tratta i dati personali per conto suo. Nonostante quello che suggerisce il nome, non risponde di nulla, non è responsabile.

9) **Destinatario:** la persona fisica o giuridica, l'autorità pubblica, il servizio, o altro organismo, a cui io comunico i dati personali.

10) **Terzo:** colui che non è né l'interessato, né il titolare, né il responsabile, né il destinatario, e che si trova ad avere l'accesso ai dati per una ragione sua particolare.

11) **Consenso:** manifestazione di volontà libera, specifica, esplicita, informata e inequivocabile dell'interessato, con la quale egli manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento.

12) **Violazione di dati personali:** databreach. Si ha quando il dato personale è stato distrutto, smarrito, modificato o divulgato senza autorizzazione. Ovvero se sia stato conosciuto da soggetti non autorizzati. Si hanno 72 ore di tempo per comunicarlo all'autorità garante, dopodiché scattano le sanzioni.

13) **Dati:**

- **Genetici:** riguardano le caratteristiche genetiche o ereditarie della persona fisica, e forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona. Sono dati molto importanti perché non cambiano nel corso degli anni.
- **Biometrici:** sono i dati più importanti in assoluto da proteggere perché non possono essere cambiati e restano univoci per tutta la vita. Quindi se vengono rubati, la mia identità digitale è a rischio.
- **Relativi alla Salute:** dati attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria che rivelano informazioni relative al suo stato di salute.
- **Orientamento e vita sessuale**

14) **Servizio della società dell'informazione:** qualsiasi servizio che riguardi la società dell'informatica e dell'informazione.

15) **Organizzazione Internazionale:** organismo di diritto internazionale."

CAPO II

Art. 5 Principi Applicabili al trattamento di dati personali (Cuore del regolamento Europeo)

a) I dati personali devono essere trattati in modo lecito, corretto e trasparente nei confronti dell'interessato (**principio di liceità, correttezza e trasparenza**).

Con liceità si intende che i dati devono essere trattati secondo le norme del regolamento.

Con correttezza che io devo essere corretto nei confronti della persona di cui sto trattando i dati, quindi devo dirgli con trasparenza come tratterò i suoi dati, quali saranno le finalità e la durata.

b) Le finalità devono essere quindi determinate, esplicite e legittime e i dati devono poi essere trattati in un modo che non sia incompatibile con tali finalità (quindi non posso dire all'interessato che tratterò i suoi dati per una determinata finalità per poi trattarli per un'altra). (**principio della limitazione delle finalità**)

c) I dati devono essere adeguati pertinenti e limitati (**principio di minimizzazione**: io devo trattare solo i dati che ho bisogno di conoscere, non di più)

d) I dati devono essere esatti e aggiornati (**principio di esattezza**)

e) I dati vanno tenuti solo per un tempo strettamente necessario allo scopo per cui li ho raccolti, dopo devono essere distrutti o resi anonimi (**principio della limitazione della conservazione**).

f) I dati vanno trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali (**principio di integrità e riservatezza**). Al regolamento non interessa come vengono protetti i dati, l'importante è che questi rimangano integri e riservati.

Principio di accountability: il titolare del trattamento non deve soltanto essere a norma, ma deve anche essere in grado di dimostrare di essere a norma (procedure, regolamenti, linee guida, schemi...). Anche qui non interessa cosa si fa nello specifico, l'importante è che sia possibile vedere che in quell'azienda il regolamento europeo viene effettivamente rispettato.

11.03.21

Nonostante l'articolo 5 sia un riassunto abbastanza dettagliato di tutto il Regolamento Europeo, ci servono anche gli articoli 6 e 9 per inquadrare in maniera più corretta possibile tutti gli aspetti affrontanti nell'articolo 5.

In particolare, l'**art. 6** spiega come trattare i **dati sensibili/comuni**, mentre l'**art. 9** i **dati particolari**.

Art. 6 Liceità del trattamento (quando un trattamento è lecito)

"Il trattamento è lecito solo se e nella misura in cui ricorre almeno una delle seguenti condizioni:

a) l'interessato ha espresso il consenso al trattamento dei propri dati personali per una o più specifiche finalità."

Art. 9 Trattamento di categorie particolari di dati personali

"È vietato trattare dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona.

Questo divieto è revocato se:

a) l'interessato ha prestato il proprio consenso esplicito al trattamento di tali dati personali per una o più finalità specifiche."

Entrambi i primi punti di questi due articoli parlano del **consenso al trattamento dei dati personali**.

Tuttavia, non basta solo avere il consenso della persona per trattare i suoi dati personali, questo perché il consenso è sempre **revocabile**: quando decido che non voglio più far trattare i miei dati posso, infatti, revocarlo.

Ecco perché sono previste altre cause di giustificazione del trattamento.

Art. 6

"b) il trattamento è necessario all'esecuzione di un contratto di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso."

Art. 9

"b) il trattamento è necessario per assolvere gli obblighi ed esercitare i diritti specifici del titolare del trattamento o dell'interessato in materia di diritto del lavoro e della sicurezza sociale e protezione sociale, nella misura in cui sia autorizzato dal diritto dell'Unione o degli Stati membri o da un contratto collettivo ai sensi del diritto degli Stati membri, in presenza di garanzie appropriate per i diritti fondamentali e gli interessi dell'interessato."

Nell'articolo 9 vengono descritti in maniera più dettagliata rispetto che nell'articolo 6.

Quindi i dati comuni gestiti dall'art. 6 hanno una regolazione meno rigida rispetto ai dati particolari gestiti dall'art. 9. Questo perché i dati particolari rischiano di causare un notevole danno all'interessato nel caso dovessero essere trattati in assenza delle opportune cautele oppure dovessero sfuggire dal controllo del titolare del trattamento.

Art. 6

"c) il trattamento è necessario per adempiere un obbligo legale al quale è soggetto il titolare del trattamento.

d) il trattamento è necessario per la salvaguardia degli interessi vitali dell'interessato o di un'altra persona fisica."

Art. 9

"c) il trattamento è necessario per tutelare un interesse vitale dell'interessato o di un'altra persona fisica qualora l'interessato si trovi nell'incapacità fisica o giuridica di prestare il proprio consenso."

Se ho un'allergia che non voglio divulgare a nessuno, posso farlo, se però dovessi essere portata al pronto soccorso e mi ritrovassi incapace di dare il mio consenso per il trattamento dei miei dati particolari che svelano la mia allergia, i dati possono essere trattati anche senza ricevere il mio consenso.

Art. 6

"e) il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento."

Per esempio se devo fare una multa ad una persona perché non indossava la cintura di sicurezza, posso trattare i suoi dati personali anche senza il suo consenso. Questo sempre considerando il **principio di minimizzazione** dell'art. 5, il quale sosteneva che posso trattare solo i dati necessari allo svolgimento del mio compito: nome, cognome, data di nascita, ecc... Non posso andare a trattare altri dati estranei al compito.

Art. 6

"f) il trattamento è necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato è un minore."

Ad esempio con i cookies: il titolare del trattamento ha interesse che il suo sito funzioni correttamente, quindi comunica all'interessato che alcuni cookies tecnici gli verranno installati non in forza di un suo esplicito consenso, ma in forza di un suo (del titolare) **legittimo interesse** al buon funzionamento del sito, quindi questi dati non avranno bisogno di consenso. L'interessato saprà della loro presenza, ma si potrà rifiutare di installarli.

Art. 9

"f) il trattamento è necessario per accertare, esercitare o difendere un diritto in sede giudiziaria o ogniqualvolta le autorità giurisdizionali esercitino le loro funzioni giurisdizionali."

A differenza dei dati comuni che possono essere trattati anche solo per il legittimo interesse, i dati particolari possono essere trattati solo per difendere un diritto in ambito giudiziario.

Art. 9

"d) il trattamento è effettuato, nell'ambito delle sue legittime attività e con adeguate garanzie, da una fondazione, associazione o altro organismo senza scopo di lucro che persegua finalità politiche, filosofiche, religiose o sindacali, a condizione che il trattamento riguardi unicamente i membri, gli ex membri o le persone che hanno regolari contatti con la fondazione, l'associazione o l'organismo a motivo delle sue finalità e che i dati personali non siano comunicati all'esterno senza il consenso dell'interessato."

Se un soggetto ha aderito ad un partito, sindacato, organizzazione religiosa, ecc., ed è in qualche modo iniziato in questa attività, egli non può pretendere che la suddetta attività lo cancelli, aggiorni i propri registri, o cancelli parte della sua storia. Finché i suoi dati vengono trattati nell'ambito dell'entità di cui stiamo parlando, il trattamento è lecito.

Art. 9

"e) il trattamento riguarda dati personali resi manifestamente pubblici dall'interessato."

Tutti i dati che rendo manifestamente pubblici da sola, ad esempio sui social.

Art. 9

"j) il trattamento è necessario a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici."

I dati devono essere proporzionali alle finalità perseguitate e devono essere bilanciati con l'interesse del soggetto rispetto all'interesse della comunità nel conoscere gli aspetti di quella storia.

Ciò è fondamentale per fare **ricerca storica** perché non possiamo farla se andiamo ad ignorare elementi della vita familiare e personale dei soggetti di cui andiamo a parlare. Questo perché, tali dati, ci danno tante informazioni sul modo in cui le persone vivevano e interpretavano tanti aspetti della vita.

Art. 10 Trattamento dei dati personali relativi a condanne penali e reati

In questo caso il trattamento dei dati personali deve essere effettuato in maniera estremamente accorta e solo se autorizzato da una legge, da uno stato. Questi **dati giudiziari** (relativi a condanne penali e reati) sono i più protetti dal punto di vista della diffusione e della divulgazione dell'informazione.

Art. 7 Condizioni per il consenso

Parla delle condizioni per cui il consenso venga validamente espresso.

1. Se il trattamento è basato sul consenso, il **titolare** deve essere in grado di **dimostrare** che l'interessato ha prestato tale consenso. Per far ciò il titolare deve essere in possesso di un **documento** che dimostri che il consenso è stato dato.

2. Se il consenso dell'interessato è prestato nel contesto di una dichiarazione scritta che riguarda anche altre questioni, la richiesta di consenso è presentata in modo chiaramente distinguibile dalle altre materie, in forma comprensibile e facilmente accessibile, utilizzando un linguaggio semplice e chiaro. Nessuna parte di una tale dichiarazione che costituisca una violazione del presente regolamento è vincolante.

3. L'interessato ha il diritto di **revocare** il proprio consenso in qualsiasi momento. La revoca del consenso non pregiudica la liceità del trattamento basata sul consenso prima della revoca.

4. Nel valutare se il consenso sia stato liberamente prestato, si tiene nella massima considerazione l'eventualità, tra le altre, che l'esecuzione di un contratto, compresa la prestazione di un servizio, sia condizionata alla prestazione del consenso al trattamento di dati personali non necessario all'esecuzione di tale contratto. (Il soggetto viene obbligato a prestare il consenso del trattamento di dati personali anche non inerenti al servizio che vuole richiedere, altrimenti tale servizio non gli viene svolto)

Art. 8 Condizioni applicabili al consenso dei minori in relazione ai servizi della società dell'informazione

Questo articolo è stato ampliato perché nella sua definizione originaria era stabilito che un soggetto al di sotto dei **16 anni** non potesse prestare il consenso per il trattamento dei propri dati personali. Ora la soglia d'età è stata abbassata a **14 anni**.

Art. 11 Trattamento che non richiede l'identificazione

Se le finalità per cui il titolare del trattamento tratta i dati personali, non richiedono o non richiedono più, di identificare l'interessato, allora egli non è obbligato a conservare, acquisire o trattare ulteriori informazioni per identificarlo al solo fine di rispettare il regolamento.

Nel caso in cui il titolare del trattamento possa dimostrare di non essere in grado di identificare l'interessato, ne informa l'interessato, se possibile.

Ad esempio, un router in un pub dovrebbe fornire l'informativa a tutti i clienti che vogliono collegarsi al WiFi, ma dal momento che questo router non si ricorderà più nulla di loro non appena questi si scollegheranno dalla rete, può evitare di farlo perché i soggetti non saranno più identificabili.

CAPO III (L'Informativa)

È regolamentata dagli articoli 12, 13 e 14.

Art. 12

"Il titolare del trattamento adotta misure appropriate per fornire all'interessato tutte le informazioni di cui agli articoli 13 e 14 e le comunicazioni di cui agli articoli da 15 a 22 relative al trattamento in forma concisa, trasparente, intelligibile e facilmente accessibile, con un **linguaggio** semplice e chiaro, in particolare nel caso di informazioni destinate specificamente ai minori. Le informazioni sono fornite per iscritto o con altri mezzi, anche, se del caso, con mezzi elettronici. Se richiesto dall'interessato, le informazioni possono essere fornite oralmente, purché sia comprovata con altri mezzi l'identità dell'interessato.

Il titolare del trattamento fornisce all'interessato le informazioni relative all'azione intrapresa senza ingiustificato ritardo e, comunque, al più tardi entro un mese dal ricevimento della richiesta stessa."

Art. 13 Informazioni da fornire qualora i dati personali siano raccolti presso l'interessato

Art. 14 Informazioni da fornire qualora i dati personali non siano raccolti presso l'interessato

- Identità e dati di contatto del titolare.
- I dati di contatto del responsabile della protezione dei dati.
- Le finalità del trattamento a cui sono destinati i dati personali.
- I legittimi interessi perseguiti dal titolare del trattamento.
- La fonte da cui hanno avuto origine i dati personali (da dove hanno preso il mio numero ad es.)
- L'intenzione del titolare di trasferire i dati in un paese terzo.
- Quanto tempo conserveranno i dati.
- Se l'interessato può chiedere al titolare del trattamento l'accesso ai dati personali e la rettifica o la cancellazione degli stessi.
- Se il trattamento è basato sul consenso, dov'è il consenso dell'interessato e dove gli è stato detto che poteva revocarlo.

Diritti degli Interessati

Art. 15 Diritto di accesso dell'interessato

"L'interessato ha il diritto di ottenere dal titolare del trattamento la conferma che sia o meno in corso un trattamento di dati personali che lo riguardano e in tal caso, di ottenere l'accesso ai dati personali e determinate informazioni."

Questo diritto consente all'interessato di sapere se il titolare abbia o meno i suoi dati personali in database e, nel caso li abbia, quali dati ha, come li conserva, per quali finalità, e se li comunica.

Art. 16 Diritto di Rettifica

"L'interessato ha il diritto di ottenere dal titolare del trattamento la rettifica dei dati personali inesatti che lo riguardano senza ingiustificato ritardo. Tenuto conto delle finalità del trattamento, l'interessato ha il diritto di ottenere l'integrazione dei dati personali incompleti, anche fornendo una dichiarazione integrativa."

Quindi l'**aggiornamento** dei dati che non sono più corretti oppure direttamente sbagliati.

(ad es. posso chiedere che i miei dati vengano aggiornati riportando il conseguimento della mia laurea)

Art. 17 Diritto alla Cancellazione (diritto all'Oblio)

"Può essere richiesto quando:

- a) i dati personali non sono più necessari rispetto alle finalità per le quali sono stati raccolti o altrimenti trattati.
- b) l'interessato revoca il consenso, a meno che la conservazione dei dati non serva al titolare per far valere un suo diritto.
- c) l'interessato si oppone al trattamento. Se non c'è un motivo legittimo prevalente per procedere al trattamento, prevale il diritto all'oblio.
- d) i dati sono stati trattati illecitamente.
- e) i dati personali devono essere cancellati per adempiere un obbligo giuridico previsto dal diritto dell'Unione
- f) i dati personali sono stati raccolti relativamente all'offerta di servizi della società dell'informazione, che non è più valida o che non richiede più il trattamento di quei dati.
- g) i dati sono stati trattati legittimamente ma è decorso un ragionevole periodo di tempo."

Non è un diritto assoluto ed è soggetto a grossi limiti.

Art. 18 Diritto di limitazione di trattamento

Quando i dati sono contestati, il garante può imporre il titolare a limitare il loro trattamento o di vincolarlo.

Art. 19 Obbligo di notifica in caso di rettifica o cancellazione dei dati personali o limitazione del trattamento

Ho la possibilità di richiedere che in caso di cancellazione o rettifica dei dati personali, questa comunicazione venga notificata a tutti i soggetti a cui sono stati comunicati i dati.

Art. 20 Diritto alla portabilità dei dati

Qualunque servizio che venga reso e che chiede una archiviazione dei dati personali, deve prevedere la possibilità di esportare i dati perché devo dare all'interessato la possibilità di portare via i suoi dati.

Art. 21 Diritto di opposizione

Posso oppormi in qualsiasi momento al trattamento dei miei dati personali, anche se basati su consenso legittimo, semplicemente revocando il consenso; oppure, nel caso non ci sia il consenso, rivolgandomi all'autorità garante per la protezione dei dati personali o all'autorità giudiziaria.

Art. 22 Processo decisionale automatizzato relativo alle persone fisiche, compresa la profilazione

Nel caso di processo decisionale automatizzato (profilazione) di un soggetto, utilizzando dati che gli appartengono, il soggetto ha il diritto di pretendere che vi sia un controllo umano volto a valutare e intervenire sul processo decisionale automatizzato. Inoltre il soggetto ha il diritto di esprimere la propria opinione o di contestare la decisione. (Es.: l'Inps non dà più la pensione ad un soggetto perché ritenuto morto, nonostante egli non lo sia)

Il soggetto ha il diritto di sapere su quali basi di dati vengono prese le decisioni che lo riguardano.

Art. 23 Limitazioni

15.03.21

CAPO IV (Titolare del trattamento e responsabile del trattamento)

Art. 24 Responsabilità del Titolare del Trattamento (Data Controller/Owner)

"il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al presente regolamento. Dette misure sono riesaminate e aggiornate qualora necessario."

Il Titolare del trattamento è l'unico responsabile del trattamento dei dati, tutti gli altri soggetti, come ad esempio il Responsabile del trattamento, non lo sono.

Per capire cosa si intende con "adeguata" bisogna fare ricorso al **principio di diligenza media** e al **principio di responsabilità oggettiva**.

Diligenza media: nell'adempimento delle sue obbligazioni il venditore deve agire con la diligenza del buon padre di famiglia, oppure, nel caso sia un professionista, con la diligenza richiesta per lo svolgimento di quelle funzioni. Ovvero quello che una persona scrupolosa normalmente farebbe per evitare l'avvenirsi di eventi dannosi.

Mentre la **diligenza straordinaria** è quella richiesta nello svolgimento di attività pericolose, cioè tutte quelle attività che hanno insito il rischio di causare un danno rilevante agli altri cittadini.

"Se ciò è proporzionato rispetto alle attività di trattamento, le misure di cui al paragrafo 1 includono l'attuazione di politiche adeguate in materia di protezione dei dati da parte del titolare del trattamento."

L'adesione ai codici (es.: codici ISO) di condotta di cui all'articolo 40 o a un meccanismo di certificazione di cui all'articolo 42 può essere utilizzata come elemento per dimostrare il rispetto degli obblighi del titolare del trattamento"

Art. 25 Protezione dei dati fin dalla progettazione e protezione dei dati per impostazione predefinita

Prevede che nel momento in cui si progetta un trattamento, è necessario progettare la sicurezza dei dati, sin dalle prime battute. Si deve partire dalla sicurezza dei dati e, sulla base di quella, costruire il trattamento. (**Privacy By Design**)

Nel momento in cui si vanno a trattare i dati, il trattamento deve essere configurato in maniera tale da trattare solamente in dati necessari, in maniera sicura, usando la pseudonimizzazione. (**Privacy By Default**)

Più dati raccolgo, più è grave la situazione in caso di databreach.

Il regolamento stabilisce che le misure di sicurezza prevedano di default, che i dati non siano accessibili a un numero indefinito di persone fisiche, senza che intervenga una determinata persona fisica a stabilire chi può o non può leggere tali dati.

Un meccanismo di certificazione approvato può essere utilizzato come elemento per dimostrare la conformità a questi requisiti.

Art. 26 Contitolari del Trattamento

Introduce la figura del Contitolare: un soggetto che tratta i dati insieme al titolare.

In questo caso va stipulato un contratto dove vengono stabilite le responsabilità dei due soggetti, e in cui si attivano dei punti di contatto.

È difficile distinguere tra Titolare, Contitolare, e Responsabile.

Contitolare VS Responsabile: se il soggetto non ha un'autonomia propria nella scelta dei dati da trattare, della finalità, e deve restituirmi i dati al termine del trattamento, stiamo parlando di un Responsabile. Perché il Contitolare gode della stessa autonomia del Titolare del trattamento.

Titolare VS Contitolare: se l'interesse è condiviso con il mio ente/titolare, abbiamo una Contitolarità, altrimenti un Titolare autonomo.

Art. 28 Responsabile del Trattamento (Data Processor)

Soggetto che tratta per conto del Titolare i dati.

Ci deve essere tra le due parti un **contratto** che abbia valore giuridico che dica al Responsabile come trattare i dati, quali dati trattare, e cosa fare con quei dati al termine dell'incarico (restituzione al Titolare, o cancellazione dei dati).

Deve esserci un **accordo di riservatezza** e il Responsabile *non* può nominare un'altra persona di svolgere il lavoro per conto suo se non esplicitamente autorizzato dal Titolare.

Il Responsabile deve anche mettere a disposizione del Titolare tutti i documenti che provano la corretta osservazione delle norme del regolamento, in caso di databreach; e deve informare immediatamente il Titolare nel caso ci sia un'istruzione che secondo lui viola il regolamento (quindi non può fare cose illegali solo perché glielo ha ordinato il Titolare, deve prima avvertirlo della violazione).

Inoltre, per tutelare i piccoli titolari da grandi compagnie:

"Se un responsabile del trattamento viola il presente regolamento, determinando le finalità e i mezzi del trattamento, è considerato un titolare del trattamento in questione."

Art. 29 Trattamento sotto l'autorità del titolare del trattamento o del responsabile del trattamento

Il trattamento viene effettuato da soggetti autorizzati, sotto la diretta autorità del Titolare o del Responsabile. Il fatto che un soggetto lavori per uno dei due, non implica che sia un soggetto autorizzato. Deve esserci una autorizzazione specifica, documentata, che gli permette di sapere quali siano le sue istruzioni.

Art. 30 Registro dei Trattamenti

Il Registro dei Trattamenti è un documento che tiene traccia di tutti i trattamenti fatti dal Titolare. Ad esempio contiene le informazioni relative: al nome e ai dati di contatto del Titolare del trattamento, le finalità del trattamento, la descrizione delle categorie di interessati o delle categorie di dati personali coinvolte nel trattamento, le categorie di destinatari a cui sono stati o a cui verranno comunicati i dati personali, i trasferimenti dei dati verso un paese terzo, i termini ultimi previsti per la cancellazione dei dati, una descrizione generale delle misure di sicurezza/organizzative previste dal regolamento, e una descrizione dei potenziali rischi per i dati. Non esiste una forma di default, può essere modificato.

Il registro può essere:

- da Titolare
- da Responsabile: tipicamente contiene meno informazioni di quello del Titolare perché il Responsabile è tenuto a comunicare, in caso di databreach, direttamente al Titolare.

Art. 32 Sicurezza del Trattamento

“Il titolare del trattamento e il responsabile del trattamento, mettono in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, che comprendono, tra le altre:

- a) la pseudonimizzazione e la cifratura dei dati personali.
- b) la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza (in grado di rinascere o continuare ad operare dopo essere stato colpito) dei sistemi e dei servizi di trattamento.
- c) la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico.
- d) avere una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento (impact analysis, vulnerability assessment, penetration test).

Il titolare del trattamento e il responsabile del trattamento fanno sì che chiunque agisca sotto la loro autorità e abbia accesso a dati personali non tratti tali dati se non è istruito in tal senso dal titolare del trattamento.”

Art. 33 Notifica di una violazione dei dati personali all'autorità di controllo

Se nonostante tutte queste misure di sicurezza, abbiamo comunque un **databreach**, dobbiamo fare una prima valutazione del danno:

- se il databreach è lieve lo annoto nel Registro dei databreach e vado avanti,

- se il **databreach** è **grave** sono tenuto a notificarlo al garante entro **72 ore**. La notifica deve contenere informazioni quali: la descrizione dell'evento, dati danneggiati, dati persi e, eventualmente, misure adottate per evitare l'impatto.
- se il **databreach** è **molto grave** e presenta un rischio elevato per i diritti e le libertà degli interessati, oltre a notificarlo al garante, dobbiamo comunicarlo anche agli interessati stessi, insieme alle misure adottate per attenuare il danno.

Questi ultimi due punti non potrò mai effettuarli entro 72 ore se non ho fatto a monte una stima dei rischi e degli eventuali danni.

Inoltre, tutte le volte che un trattamento presenta dei rischi specifici, bisogna fare una valutazione di impatto (Privacy Impact Assessment), con la quale si analizzano tutti i singoli trattamenti a rischio dell'ente, stabilendo quanto sono a rischio e quanto le misure di sicurezza vanno ad impattare sul rischio. Se il rischio rimane elevato, ciò va comunicato al **garante**, il quale può: consentirmi di effettuare comunque il trattamento, di effettuare il trattamento con ulteriori misure di sicurezza, oppure può impedirmi di effettuare il trattamento.

18.03.21

Art. 37 Designazione del responsabile della protezione dei dati (Data Protection Officer DPO)

Il **Responsabile della protezione dati personali** è una posizione quasi paritetica a quella del Titolare, pur essendo un subordinato di esso. Egli ha infatti una funzione essenziale di **consulenza e assistenza al Titolare**, e dovrebbe poter svolgere le sue attività in completa **autonomia**. Ha il compito di far capire al titolare che i dati possono essere trattati in maniera più sicura e accorta, portando un guadagno sia in termini di tempo che in termini di riduzione del carico di lavoro.

Il **Titolare del trattamento** deve rendere nota l'identità del DPO all'autorità di controllo e ai suoi interessati, ecco perché il regolamento europeo prevede l'obbligo di **pubblicare i dati di contatto** del DPO.

"Il titolare del trattamento e il responsabile del trattamento nominano obbligatoriamente un responsabile della protezione dei dati ognqualvolta:

- a) **il trattamento è effettuato da un'autorità pubblica o da un organismo pubblico (università, regione, stato, comuni, province...)**
- b) **le attività principali del titolare del trattamento o del responsabile del trattamento consistono in trattamenti che, per loro natura, ambito di applicazione e/o finalità, richiedono il monitoraggio regolare e sistematico degli interessati su larga scala (Amazon, Bartolini, America Express)**
- c) **le attività principali del titolare del trattamento o del responsabile del trattamento consistono nel trattamento, su larga scala, di categorie particolari di dati personali o di dati relativi a condanne penali e a reati (dati giudiziali)"**

Art. 38 Posizione del responsabile della protezione dei dati

"Il titolare del trattamento e il responsabile del trattamento devono garantire che il responsabile della protezione dei dati sia tempestivamente e adeguatamente coinvolto in tutte le questioni riguardanti la protezione dei dati personali"

È il titolare che deve garantirlo, non è il DPO che deve costantemente informare il titolare. È il titolare che deve rivolgersi al DPO e informarlo di ogni nuovo trattamento.

"Il titolare e del trattamento e il responsabile del trattamento sostengono il responsabile della protezione dei dati nell'esecuzione dei compiti fornendogli le risorse necessarie per assolvere tali compiti e accedere ai dati personali e ai trattamenti e per mantenere la propria conoscenza specialistica."

In poche parole il DPO deve essere **pagato**.

"il responsabile della protezione dei dati non riceva alcuna istruzione (indicazioni/ordini) per quanto riguarda l'esecuzione di tali compiti."

In modo che il DPO non diventi una marionetta nelle mani del Titolare. È il DPO che deve dire al titolare come deve essere fatto il trattamento, altrimenti il suo ruolo diventa inutile.

"Gli interessati possono contattare il responsabile della protezione dei dati per tutte le questioni relative al trattamento dei loro dati personali.

Il DPO è tenuto al segreto o alla riservatezza in merito all'adempimento dei propri compiti.

Il responsabile della protezione dei dati può svolgere altri compiti e funzioni purché essi non diano adito a un conflitto di interessi."

Art. 39 Compiti del responsabile della protezione dei dati

"Il responsabile della protezione dei dati è incaricato almeno dei seguenti compiti:

- a) informare e fornire consulenza al titolare o al responsabile nonché ai dipendenti.
- b) sorvegliare l'osservanza del presente regolamento. Quindi vanno fatti degli audit o interviste, per verificare che il regolamento venga effettivamente osservato e che sia tecnicamente rispettato.
- c) fornire, se richiesto, un parere in merito alla valutazione d'impatto sulla protezione dei dati e sorveglierne lo svolgimento
- d) cooperare con l'autorità di controllo. Il DPO non è una spia che deve comunicare all'autorità di controllo tutto ciò che succede nell'azienda (non devono segnalare eventuali illeciti), deve solo cooperare con essa per fargli capire perché si sono svolte certe attività, perché certe procedure per lui sono corrette e perché si sono fatte certe scelte.
- e) Nell'eseguire i propri compiti il responsabile della protezione dei dati considera debitamente i rischi inerenti al trattamento, tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del medesimo."

CAPO V

Questa sezione parla di Codici di condotta e di certificazione, e dice essenzialmente che possono essere utilizzati per presentare e dimostrare in sede di accertamento che vengano rispettate certe procedure.

Art. 44 Principio generale per il trasferimento dei dati all'estero

Nel momento in cui trasferisco dati all'estero devo rispettare una serie di principi, che siano conformi con il regolamento.

I dati possono essere portati all'estero sulla base di 3 ragioni...

Art. 45 Trasferimento sulla base di una decisione di adeguatezza

Sono direttamente i garanti Europei che ci dicono che quel determinato paese è adeguato.

Art. 46 Trasferimento soggetto a garanzie adeguate

Adequate garanzie di protezione dei dati da parte del destinatario.

Art. 47 Norme vincolanti d'impresa

Norme che garantiscono che quei dati saranno protetti.

CAPO VIII

Art. 83 Condizioni generali per infliggere sanzioni amministrative pecuniarie

Il garante valuta:

- a) la modalità con cui è stata commessa l'infrazione, quindi il carattere **doloso o colposo** dell'infrazione (volontariamente o per puro errore),
- b) la natura, la gravità e la durata dell'infrazione,
- c) le misure adottate dal Titolare o dal Responsabile per attenuare il danno subito dagli interessati,
- d) Il grado di responsabilità del Titolare o del Responsabile tenendo conto le misure di sicurezza e organizzative messe in atto,
- e) Eventuali precedenti violazioni,
- f) Le categorie di dati personali interessate,
- g) Come l'autorità di controllo è venuta a sapere del databreach: gliel'ho detto io entro le 72 ore, o lo è venuta a sapere da sola?
- h) Se sono stati violati certi provvedimenti del garante che dicevano come effettuare un determinato trattamento,
- i) Se sono stati di rispettati i codici condotta a cui avevo aderito,
- j) Se il danno è stato causato da una mia ricerca di un interesse personale, di un guadagno. (in questo caso la sanzione aumenta ovviamente).

Sanzioni:

- Per infrazioni lievi: arriva fino 10 milioni di euro o al 2% del fatturato mondiale annuo,
- Nel caso di violazioni del principio del consenso, i diritti degli interessati, il trasferimento dei dati all'estero: fino a 20 milioni di euro o il 4% del fatturato mondiale annuo.

Classificazione dei soggetti

Classificazione a piramide: dall'alto verso il basso abbiamo rispettivamente i soggetti più importanti, fino ad arrivare a quelli di minore importanza. I responsabili, sub-responsabili e il DPO fanno parte di strutture gerarchiche distinte rispetto a quella del titolare.

Titolare	Responsabili: soggetti che trattano i dati per conto del titolare senza però far parte della struttura gerarchica del titolare.	DPO
Soggetti designati: coloro che il titolare ha autorizzato a trattare i dati personali in suo nome e per conto.	Sub-responsabili: soggetti responsabili dei responsabili. Trattano dati per conto dei responsabili, ma è il responsabile a rispondere del trattamento.	
Soggetti autorizzati al solo trattamento: coloro che possono solo vedere i dati che devono inserire/trattare		

Internet ha vari strati.

Il **Surface Web**, uno strato di apparenza, costituito da siti web, pagine e servizi. È quello che noi pensiamo di vedere di internet, ed è ciò a cui possiamo accedere utilizzando i motori di ricerca.

I motori di ricerca, infatti, lavorano sulla superficie di internet.

Il **Deep Web**, invece, è tutta quella parte di internet che non viene indicizzata dai motori di ricerca. Questo per diverse ragioni:

- perché si tratta di pagine private,
- contenuti che *non* possono essere tecnicamente indicizzabili, come ad esempio le pagine dinamiche che sono costruite sulla base della scelta degli utenti
- pagine che possono essere raggiunte solo da link realizzati in JavaScript o in Flash e che hanno quindi contenuti non testuali non indicizzabili dai motori di ricerca.
- pagine bandite.

Quando parliamo di **pagine private**, parliamo di:

1. pagine ad accesso ristretto (es.: pagine di posta elettronica).
2. pagine a pagamento (es.: banche dati dei giornali).
3. pagine il cui accesso ai motori di ricerca viene bloccato per ragioni legali.

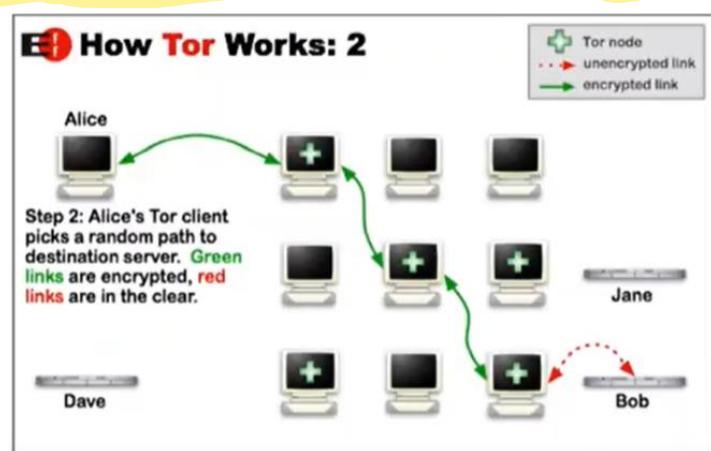
Il **Dark Web (Dark Net)** è quella parte della rete che può essere raggiunta esclusivamente utilizzando appositi strumenti: peer to peer (es.: Emule, Torrent), Tor.

Le darknet sono pericolose perché sfuggono al controllo delle autorità, pullulano di contenuti illegali e, a volte, coloro che hanno contenuti in questa parte di internet non amano i curiosi, quindi non è bene lasciare troppe informazioni in giro che possano identificare. Tuttavia, esse nascono con uno scopo nobilissimo, ovvero quello di permettere a chi vive in paesi dove c'è la censura, di potersi collegare a fonti pubbliche e diffondere informazioni senza rischiare la vita. Hanno quindi un ruolo fondamentale nella Libertà di Parola e nel diritto di Libertà degli individui.

Per navigare con Tor spesso si utilizza un **portale di partenza** (generalmente la Hidden Wiki), oppure un motore di ricerca (DuckDuckGo) che però non sono efficaci come i motori di ricerca classici per il Surface Web, proprio perché molti dei siti che fanno parte delle Darknet non vogliono farsi trovare.

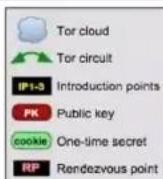
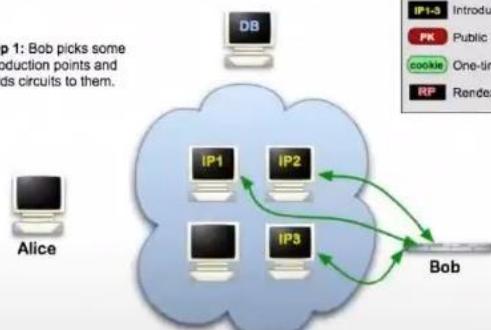
Tor è una **catena di proxy** che ha due funzioni principali: la riservatezza, permettendo un collegamento in maniera anonima ad un sito di superficie, e la possibilità di collegarsi ad una dark net per raggiungere i così detti hidden services.

I servizi di Tor funzionano con i **randevouz point**: non mi collego direttamente da A a B, ma utilizzo una serie di nodi che mi portano alla destinazione. In questo modo B non conoscerà mai l'indirizzo IP di A. Quindi B vedrà solamente l'indirizzo IP dell'ultimo nodo che gli ha passato la connessione, così come l'ultimo nodo vedrà solo quello del nodo precedente, e così via.



Tor Hidden Services: 1

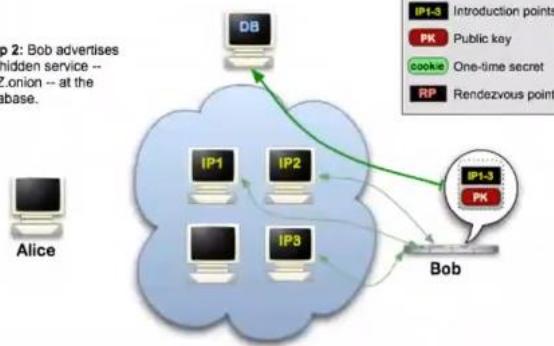
Step 1: Bob picks some introduction points and builds circuits to them.



Ogni tot di minuti, inoltre, il percorso tra i nodi cambia in maniera casuale, così da evitare attacchi diretti all'individuazione dei nodi.

Tor Hidden Services: 2

Step 2: Bob advertises his hidden service -- XYZ.onion -- at the database.



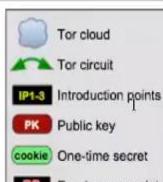
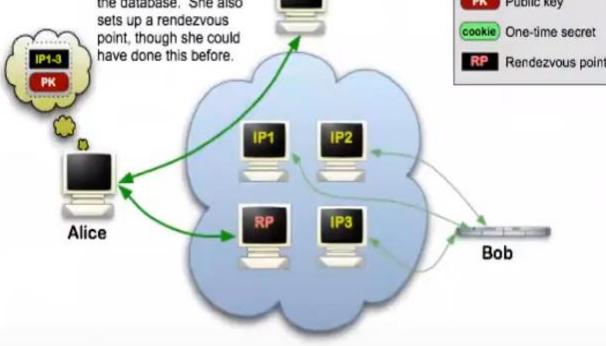
Quando parliamo di **hidden services**, però, questo implica una sosta all'interno della Darknet.

- [1] Prima di tutto mi collego con un introduction point.
- [2] Dopodichè mi collego ad un server centrale che ha la funzione di manifesto, e gli comunico l'indirizzo del mio server che in questo modo potrà essere raggiunto.
- [3] Quando qualcuno vuole connettersi al mio servizio, deve conoscere l'indirizzo e, dopo averlo digitato all'interno di Tor, il browser si collega al database che funge da DNS e lo reindirizza al rendezvous point, un terzo server in cui convergono le informazioni.

Tutti questi passaggi sono necessari affinché non solo il server non saprà chi si collega a lui, ma coloro che si collegano al server non sapranno dove si trova anch'esso. Massimo livello di riservatezza.

Tor Hidden Services: 3

Step 3: Alice hears that XYZ.onion exists, and she requests more info from the database. She also sets up a rendezvous point, though she could have done this before.



25.03.21

Servizi Dark Web

1. **Servizio di Hosting:** vengono forniti per garantire la possibilità di creare siti web completamente anonimi. Non sono essenzialmente siti illegali, ma comunque fanno sì che diventi estremamente difficile risalire all'identità del soggetto che ha creato il sito.

Tutti questi siti hanno caratteristiche e prestazioni ridotte rispetto ai siti del Surface Web, perché è molto

più costoso gestire un tale servizio nel Dark Web e perché questi siti dispongono di meno spazio (circa 2GB).

2. **Servizio di E-Commerce:** identico a quelli del Surface Web, con l'unica differenza della merce venduta che in questo caso è illegale: droga, armi, documenti falsi... Inoltre, la valuta è espressa in Bitcoin.
3. **Servizi di Comunicazione:** che consentono di inviare un messaggio con la garanzia che esso verrà distrutto dopo essere stato letto e che non potrà essere acquisito tramite screenshot.
Ci sono altri servizi di messaggistica che mettono a disposizione una casella di posta temporanea, la quale scomparirà dopo 10 minuti, così da garantire la riservatezza dei nostri indirizzi di posta elettronica.
4. **Wiki:** guide dedicate ai più svariati argomenti, legali e illegali.

5. **Social Network e Forum**: generalmente con contenuti illegali (hackeraggio e terrorismo).
6. **RedRoom**: torture e uccisioni live, che si paga per guardare o essere il Master della sessione.
7. **Terrorismo**: siti dedicati al reclutamento per il terrorismo, per la propagazione di notizie terroristiche, e sia per attività di cyberwar e cyberterroismo fatti attraverso il web.
8. **Hacktivism**: hacking indirizzato al contrasto delle operazioni/associazioni illegali. Bisogna stare attenti perché determinate operazioni di hacktivism sono illegali anche se sono effettuate per scopi nobili.

Decloaking

Il Decloaking è l'attività di contrasto alle informazioni illegali del Dark Web, che viene portata avanti con vere e proprie operazioni di hacking, volte ad individuare i soggetti che si nascondono dietro ai server. Generalmente vedono coinvolti il Dipartimento di Giustizia Americano, FBI, Interpol e Europol.

Bitcoin

01.04.21

Il Bitcoin è una **criptovaluta**, una **valuta virtuale** (e non fiat: prodotta da uno stato sovrano), che sta alla base della Blockchain.

La **Blockchain** nasce per risolvere il problema del **Double Spending**, ovvero impedire ad una persona di spendere due volte le stesse monete. Essa è infatti un **registro delle transazioni** e delle operazioni compiute utilizzando i Bitcoin.

Il Bitcoin a livello giuridico non offre **nessuna garanzia**, è una forma di pagamento e di scambio equiparabile al baratto. Se si comprano dollari, euro, yen, ecc., o qualsiasi altra valuta riconosciuta a livello internazionale, invece, ho alle spalle una banca centrale che garantisce il valore di tale valuta.

Non è una **valuta anonima**, come molti pensano, perché potendo vedere tutte le transazioni avvenute nella Blockchain, posso ricostruire tutto il percorso e ricondurle ad un soggetto. È una **valuta riservata**. Per ovviare al problema dell'anonymità, sono nati i **dark wallet**: wallet bitcoin che consentono di applicare sistemi di anonymizzazione e di mixing applicando vari strumenti alla transazione così da non rendere riconoscibile l'origine del mittente e del destinatario. Oppure si possono usare delle **washing machine** online (tipicamente negli hidden services) che lavorano utilizzando il principio del **mixing**: sito che prende i miei bitcoin li mette insieme a quelli di altre persone, li rimescola e li mette in un altro wallet, applicando anche principi di randomizzazione al trasferimento dei fondi (possono aspettare un numero random di minuti prima di ricacciare i soldi, così da non renderla direttamente collegabile a chi ha appena immesso i bitcoin nella washing machine. Inoltre il trasferimento della somma non avviene nella sua interezza, ma in più trasferimenti di somme minori, più una commissione di costo randomico).

Il Bitcoin è un'**operazione matematica** che mi permette di pagare utilizzando un **codice alfanumerico** (indirizzo del wallet) e non mi da nessuna garanzia che il mio pagamento sarà accettato.

Rappresenta una forma di guadagno molto facile, ma allo stesso tempo è una forma di **scommessa estremamente pericolosa** perché, se domani tutti i servizi dovessero decidere di non accettare più pagamenti con questa valuta, essa si svaluterebbe completamente.

I Bitcoin devono essere **minati**, cioè devono subire una procedura per poter essere coniati, che ne garantisca la **irripetibilità** e la **validità**.

Come si può evitare che girino Bitcoin falsi? Rendendo il falso meno conveniente dell'originale: la cosiddetta **Proof Of Work**. Se per garantire la validità di una moneta, si crea una Proof Of Work simile a quella necessaria per ottenere una moneta lecita, a quel punto c'è la certezza che le mie monete non vengano falsificate. Perché la falsificazione della moneta richiederebbe un lavoro eccessivo rispetto al beneficio/guadagno che se ne ricaverebbe.

L'**HashCash** è una sorta di francobollo virtuale in base al quale devo risolvere un **piccolo esercizio matematico**, che richiede un determinato lasso di tempo trascurabile per un singolo messaggio, ma che diventa impraticabile per milioni di messaggi; mentre colui che lo riceve ha bisogno di un secondo per verificarlo.

Più zeri aggiungo a sx di questo hash, più il calcolo diventa complicato, ecco perché i minatori di Bitcoin stanno acquistando tantissime schede video: per avere computer con una potenza di calcolo abbastanza elevata da risolvere tali problemi.

Il Bitcoin è nato nel **2008** e venne utilizzato nella sua prima transazione per acquistare una birra e due pizze il 18 Maggio 2010, al costo di 10.000 Bitcoin (550 milioni di euro oggi).

Per incentivare i soggetti che minano, viene riconosciuto un **reward** al primo soggetto che mina un blocco, ecco anche perché l'attività di mining è molto competitiva. Chiunque finisce di minare il blocco per primo si accaparra il premio, mentre gli altri non ricevono nulla. Quindi il lavoro non è automaticamente destinato a fruttare.

Ecco perché è considerato una valuta **non Ecosostenibile** perché c'è una perdita di energia, di tempo macchina, di denaro e risorse ambientali, enormemente superiore a quello che è il guadagno che garantisce il mining di un Bitcoin.

Esistono due tipi di Blockchain: accanto alla Blockchain come registro distribuito, pubblico, immodificabile e immutabile, **permissionless** cioè senza nessun controllo o verifica se non la **Proof of Work** (quindi completamente trasparente e democratica), esistono anche altre Blockchain **permissioned** che mettono la sicurezza della Blockchain nelle mani di pochi soggetti fidati (trusted) i quali dovrebbero essere in grado di garantire la validità di tutte le transazioni (**Proof of Stake**, stakeholder, di possesso. Generalmente un soggetto più monete ha, più è interessato che la Blockchain funzioni correttamente). Questo vuol dire che se non ci si fida degli utenti trusted, il sistema della Blockchain cade, perché questi soggetti possono falsificare la Blockchain. Se però ci si fida, abbiamo un sistema molto più flessibile e riservato rispetto alla Blockchain permissionless, perché posso nascondere i dati all'interno delle transazioni non rendendoli trasparenti.

Se il **50%+1** dei nodi di una permissioned Blockchain è affidabile, la Blockchain è affidabile.

Non essendoci una **borsa ufficiale** per il Bitcoin, abbiamo prezzi diversi (a seconda del servizio che sceglio) ai quali comprare o vendere Bitcoin. Quindi il Bitcoin vale quello che noi siamo disposti a pagare per averlo, in caso di acquisto, mentre in caso di vendita vale quanto la nostra controparte è disposta a pagare per averlo. Tutto ciò è perché non è una valuta ufficiale. Se, infatti, con gli euro non posso dire che per me 50€ valgono 10€, con i Bitcoin non c'è nessuno che mi costringe ad accettare il valore nominale del Bitcoin.

Un blocco della Blockchain non è altro che l'insieme di informazioni contenute all'interno di un "foglio" in cui viene detto chi ha fatto cosa. Ogni blocco contiene una serie di transazioni, l'hash del blocco, l'ora in cui è stato minato, le sue dimensioni, il Miner che l'ha minato, il livello di difficoltà, il reward, il **fee reward** (premio per le commissioni di transazione), il **Nonce** (numero che il miner deve indovinare perché tutto il blocco dia l'hash riportato sopra). In pratica tutta l'attività di mining consiste nell'inserire nel blocco un numero che gli permetta di avere un hash al di sotto del valore riportato. In termini tecnici il mining è un Brute Force Attack.

Ogni 4 anni il **reward viene dimezzato** quindi il guadagno di bitcoin tramite reward raggiungerà lo zero,

cosa che comporterà il raggiungimento di un **CAP**, cioè di un numero di Bitcoin massimo. Questo per contenere un rischio di inflazione.

La Blockchain funziona nel seguente modo:
ogni blocco ha al suo interno, oltre al timestamp, l'hash del blocco precedente. È per questo motivo che la Blockchain non può essere modificata e falsificata; perché, se falsifico il blocco 2 dopo che è stato minato il blocco 3, ci vorrebbe un impegno grandissimo per modificare tutti i blocchi successivi al 2. Impegno che non varrebbe il guadagno.



Per minare non è importante avere solo un hardware adeguato (asic) ma anche un **software adeguato** che deve essere in grado di interfacciarsi con la Blockchain, con i dispositivi e i sistemi che usiamo per minare, e deve essere performante.

Browser Mining: attività che utilizza il browser dell'utente per minare Bitcoin. Uno script viene installato sulla macchina dell'utente e, in cambio della fruizione del servizio, mina Bitcoin. Il servizio viene pagato tramite il mining di Bitcoin.

Se ciò non è fatto onestamente, però, posso far sì che la CPU dell'utente sia interamente dedicata al mining, bloccandogli così il computer. È quindi un'attività legale se c'è il **consenso** della persona e se è chiaro e evidente all'utente che sta avvenendo il mining. Altrimenti è reato.

Altre Criptovalute

Il Bitcoin non è l'unica criptovaluta:

- **Monero:** criptovaluta molto aggressiva destinata a sostituire il Bitcoin in tutti i Dark Market, perché a differenza del Bitcoin, Monero è anonimo. Se, infatti, per avere la non tracciabilità con i Bitcoin dobbiamo avere un Dark Wallet, Monero ha già tutto di default nativamente.
Ha un CAP differente rispetto al Bitcoin, ha un blocco ogni 2 minuti invece che ogni 10 minuti, utilizza l'algoritmo CryptoNight (Bitcoin utilizza CryptoNote).
- **Ripple:** è un sistema di trasferimento di fondi in tempo reale che permette la spedizione di denaro grazie a un servizio garantito dall'omonima società, ed è basato su un protocollo open source. Usa il protocollo SMTP per trasferire il denaro perché vuole mantenersi molto semplice, veloce ed economico, in grado di scambiare soldi anche tra diversi sistemi bancari.
Richiede un importo minimo per transazione in modo da evitare attacchi DOS.



Lezione riassuntiva e di chiarimento degli argomenti. In particolare: Registro del trattamento, Mining e Blockchain.

Smart Contract

03.05.21

Quando parliamo di Smart Contract parliamo della caratteristica dei contratti di sapersi adattare automaticamente alle esigenze dei contraenti (da qui il termine 'smart'). Non sono (solo) contratti automatici, o contratti a distanza classici, ma sono dei contratti in grado di auto-aggiornarsi. L'idea alla base dello Smart Contract è quella di sostituire all'intervento umano, una gestione del contratto completamente affidata alla macchina.

La differenza con i contratti automatici sta nel fatto che questi sono contratti predefiniti con algoritmi semplici (if-then), mentre gli Smart Contract sono in grado di evolversi e di prevedere degli adattamenti ai comportamenti delle parti.

Ad esempio, uno Smart Contract, è in grado di variare il premio dell'assicurazione in base sullo stile di guida del conducente.

Gli Smart Contract mi permettono quindi di porre in essere tutta una serie di condizioni flessibili, la cui difficoltà non sta tanto nel prevederle, quanto nel verificarne l'esecuzione (è l'apparecchio stesso che le verifica).

Condizione del contratto: evento futuro ma incerto (es.: Se arriverà la nave dall'America ti venderò 10 tonnellate della merce).

Termine del contratto: evento futuro e certo (es.: quando arriverà Natale, ti venderò 10 tonnellate della merce).

Gli Smart Contract non nascono con Ethereum, sono stati pensati ancor prima di lui e di Bitcoin, ma sicuramente con esso fanno un passo in avanti perché è un linguaggio espressamente pensato per questo tipo di contratti.

Ethereum, infatti, più che una valuta, è un sistema di gestione di Smart Contract sviluppato tra il 2013 e il 2014.

Nasce come una Blockchain in grado di integrare al suo interno un linguaggio di programmazione Turing completo, ovvero un linguaggio che consente di utilizzare tutte le sue istruzioni in modo da essere molto più flessibile e completo dei classici linguaggi usati ad esempio per i Bitcoin. È un linguaggio che consente tutte le varianti possibili e ipotizzabili di un linguaggio di programmazione e viene applicato attraverso i 4 campi tipici contenuti da un account Ethereum:

- **Nonce**: utilizzato per assicurarsi che la transazione possa essere elaborata una sola volta.
- **Ether Balance**: conto corrente dell'account, la capacità dell'account di ricevere e di effettuare pagamenti.
- **Contract Code**: codice contratto dell'account.
- **Storage**

Per poter girare sulla rete Peer-To-Peer di Ethereum, i contratti devono pagare una **fee** usando un'unità di conto chiamata Ether, la quale funge sia da criptovaluta che da carburante.

L'obiettivo di Ethereum non era tanto quello di creare una criptovaluta, ma quello di creare un **sistema/infrastruttura** di alto livello per lo sviluppo degli Smart Contract e delle transazioni tra macchine.

Gli account Ethereum possono essere di 2 tipi:

1. **Account Esterini**: account controllati da chiavi private che non contengono codice, e possono essere utilizzati per inviare e ricevere messaggi, quindi creando e firmando ogni transazione.
2. **Account Contratto** (Contract Account): controllati da un codice contratto in modo che ogni volta che il codice contratto riceve un determinato messaggio, si attivi, permettendogli di leggere e scrivere attraverso uno storage interno, di spedire altri messaggi o di creare ulteriori contratti attraverso un sistema nidificato che permette una flessibilità infinita dell'aspetto contrattuale.

Il contratto Ethereum (Smart Contract) richiede di essere integrato nel nostro **Codice Civile**.

Questo non è un problema perché il codice civile, a differenza del codice penale, consente il ricorso ad uno strumento che si chiama **analogia**: un principio giuridico per cui a casi simili si applicano norme simili.

Quindi si possono applicare allo Smart Contract gran parte delle discipline e previsioni già contenute nel Codice Civile.

Per fare questo, però, devo essere in grado di interpretare il codice sorgente del contratto, cosa che costituisce uno dei più grossi problemi all'implementazione degli Smart Contract. Mentre, infatti, un contratto normale potrebbe essere letto da chiunque, uno Smart Contract non ha questa caratteristica. Il testo leggibile scritto nel **linguaggio comune**, non è quello che fa funzionare realmente il contratto, ma è un **linguaggio macchina Turing**.

Uno dei primi problemi degli Smart Contract è quindi quello di verificare che il linguaggio umano e il linguaggio macchina coincidano, utilizzando un **convertitore/traduttore** che mi consenta di verificare che le clausole contrattuali che vado a firmare siano quelle effettivamente contenute nel mio codice sorgente. In caso di **bug**, quindi, devono esserci delle norme in grado di gestire le **responsabilità e le patologie** relative ad uno Smart Contract.

Per fare ciò dobbiamo immaginare questo contratto come un **rapporto di rappresentanza** tra il committente, il programmatore e la macchina. Nonostante, infatti, manchino due soggetti distinti come invece abbiamo nei rapporti di rappresentanza classici, possiamo comunque applicargli dei principi simili: il computer ha la stessa volontà di colui che gli impedisce le istruzioni, tuttavia potrebbe anche avere comportamenti differenti a causa di errori di programmazione.

- **Errore Ostativo**: ho sbagliato a scrivere. (**Art. 1433 Codice Civile**)
- Volontaria **Manomissione** del programma in modo tale da indurlo a commettere quello specifico errore. Può essere posta in essere da uno dei due contraenti o da un terzo soggetto. (**Art. 1439 Codice Civile**)
- Errore su un **elemento essenziale** del contratto o a causa dell'errore dell'elaborazione delle informazioni, oppure per un errore nell'inserimento delle informazioni necessarie alla macchina per l'elaborazione (**Art. 1428 Codice Civile**, gestione dell'errore del rappresentante)

Tutte queste situazioni vanno alleggerite ricorrendo all'**Art. 1390 del Codice Civile**, rivolto a gestire, analizzare e ridurre la portata degli errori del Rappresentante: il **contratto è annullabile** se viziata la volontà del rappresentante; tuttavia quando il vizio riguarda elementi predeterminati dal Rappresentato (cioè dal Dominus) il contratto è annullabile solo se era viziata la volontà del Dominus.

Come funziona il **codice del contratto**: il codice utilizzato alla base di Ethereum è un linguaggio di basso livello (**Ethereum Virtual Machine Code – EVM Code**). L'EVM è una **macchina virtuale** ideata per essere eseguita da tutti i partecipanti di una rete peer-to-peer ed è in grado di leggere e scrivere su una blockchain sia codice eseguibile che dati. È in grado di verificare le firme digitali alla base dei vari contatti ed eseguire le istruzioni.

Ha 3 grandi ambiti di applicazione:

1. **Applicazioni Finanziarie**: che forniscono agli utenti vari modi per gestire i contratti, ad esempio su monete, derivati finanziari, libretti di risparmio, testamenti, ecc...

2. **Applicazioni Semi Finanziarie:** dove il denaro è coinvolto, ma vengono coinvolti in maniera pesante anche aspetti non strettamente monetari, come per esempio l'assegnazione di premi per risolvere problemi computazionali.
3. **Applicazioni Non Finanziarie:** come ad esempio quelle finalizzate a gestire il voto online, il governo decentralizzato, o strumenti diretti di democrazia partecipata.

La prima base di Smart Contract è un concetto quasi filosofico predisposto parecchi anni fa (anni 70-80) dove si ipotizzava un contratto in cui siano presenti 3 elementi:

1. Un **Codice**: che diventa espressione della logica contrattuale.
2. **Eventi**: che il programma è in grado di acquisire e che vanno ad interagire col contratto.
3. **Effetti**: che vengono determinati dagli eventi.

Quindi per avere uno Smart Contract, dobbiamo avere un codice in grado di **interagire con**, e **interpretare**, la **realtà**. Ecco perché, ad oggi, gli Smart Contract hanno applicazione solo in quegli scenari dove è facile prevedere determinate situazioni (assicurazioni, banche e istituti finanziari).

Lo Smart Contract è un **contratto scritto** che può essere stipulato o da soggetti entrambi presenti nel luogo, oppure a distanza come accade nei contratti telematici.

Come il mondo dell'informatica venga regolamentato dal Codice Penale.

Differenza tra reato fisico che chiede un determinato impegno, rispetto ad uno informatico che richiede un **coinvolgimento emotivo** molto minore da parte del soggetto agente dato che si trova ad agire non con una persona fisica ma con una sua trasposizione virtuale.

Il reato informatico ha quindi il grosso vantaggio per l'autore di essere **immateriale** e di non richiedere l'interazione con la vittima.

Ciò non vuol dire che il reato informatico sia meno grave e abbia conseguenze minori rispetto a quello fisico.

Dobbiamo fare una prima distinzione tra:

- **Reati Informatici in senso stretto (propri)**: tutti quei reati che non potrebbero esistere se non esistesse l'informatica. Il computer è elemento necessario perché si possa parlare di questo tipo di reato.
- **Reati Informatici in senso lato (impropri)**: tutti quei reati per cui i computer hanno dato nuovi strumenti per compiere azioni che già si potevano compiere senza di essi. Il computer rende il tutto più comodo. Trasposizione informatica di reati fisici. Quasi qualsiasi reato presente nel Codice Penale può avere la sua controparte informatica, dai reati di falso ai reati di violenza.

Rientrano nei reati informatici anche le **Cyber War** e il **Cyber Terrorismo**: ormai tutti gli eserciti si muovono nella quinta dimensione.

La Cyber War può andare ad attaccare gli organi vitali delle infrastrutture nemiche: i centri di comunicazione, i centri di comando, ecc...

Più uno strumento informatico è facile da usare, più è facile da hackerare.

Reati contro la persona: tutti quei reati che hanno ad oggetto la salute, la sicurezza, l'incolumità fisica, l'onore e la reputazione, di un soggetto.

Reati contro il patrimonio: tutti quei reati che hanno ad oggetto un impoverimento del patrimonio della persona.

Il confine tra i due è molto labile, perché molto dipende dalla volontà e l'intenzione del soggetto agente. Ad esempio: un attacco ad un pacemaker con l'intento di uccidere una persona, rientra nei reati contro la persona perché voglio minare la sua salute; mentre un attacco ad un pacemaker in fase di produzione, è un reato contro il patrimonio perché finalizzato a non far approvare un prodotto o a danneggiarlo, per arrecare un danno economico all'azienda.

Le principali norme relative ai reati informatici:

1. Quelle che proteggono la riservatezza delle informazioni
2. Quelle che proteggono la sicurezza delle infrastrutture
3. Quelle che proteggono la veridicità in esse contenuti

Riservatezza delle Informazioni

Qualsiasi tipo di comunicazione che intercorra tra due sistemi informatici, analogici o di altro genere, rappresenta una comunicazione/corrispondenza.

Questo significa che l'invio di un SMS è considerato corrispondenza, tanto quanto l'invio di un messaggio tramite piccione viaggiatore.

L'Art. 616 e seguenti del Codice Penale, proteggono l'inviolabilità dei segreti.

Art. 616 -Codice Penale

In particolare protegge la **corrispondenza**, ovvero qualunque tipo di comunicazione epistolare, telefonica, telegrafica, informatica o telematica, cioè effettuata con qualsiasi altra forma di comunicazione a distanza.

Art. 15 -Costituzione

Protegge la corrispondenza dicendo che: la liberà e la segretezza della corrispondenza e di ogni altra forma di comunicazione, sono inviolabili.

Quindi io non posso visualizzare o cancellare una corrispondenza/messaggio non diretto a me.

Il Codice Penale dice infatti:

"Chiunque prende cognizione del contenuto di una corrispondenza chiusa, a lui non diretta, ovvero la sottrae o la distrae al fine di farne perdere da altri cognizione, ovvero la distrugge o sopprime, è punito con la reclusione fino a un anno e con una multa da euro 30 a euro 516.

Se il colpevole, senza giusta causa, rivela in tutto o in parte il contenuto della corrispondenza, è punito con la reclusione fino a 3 anni."

Art. 617 e 617bis -Codice Penale

Riguardano la cognizione, interruzione o impedimento illeciti, di comunicazioni telegrafiche o telefoniche. Il 617bis riguarda l'installazione di apparecchiature atte ad intercettare o impedire comunicazioni telegrafiche o telefoniche. È tuttavia lecito registrare le proprie telefonate senza dire nulla a nessuno (senza l'utilizzo di tale registrazione), mentre è illecito non registrare comunicazioni in cui non partecipo (intervettazione abusiva).

"Chiunque fraudolentemente, prende cognizione di una comunicazione o di una conversazione, telefoniche o telegrafiche, tra altre persone o comunque a lui non dirette, ovvero le interrompe o le impedisce è punito con la reclusione da sei mesi a quattro anni."

"Chiunque fuori dei casi consentiti dalla legge, installa apparati, strumenti, parti di apparati o di strumenti al fine di intercettare od impedire comunicazioni o conversazioni telegrafiche o telefoniche tra altre persone è punito con la reclusione da uno a quattro anni."

Art. 617-ter -Codice Penale

Aggiunge anche la falsificazione.

"Chiunque, al fine di procurare a sé o ad altri un vantaggio o di recare ad altri un danno, forma falsamente, in tutto o in parte, il testo di una comunicazione o di una conversazione telegrafica o telefonica ovvero altera o sopprime in tutto o in parte il contenuto di una comunicazione o di una conversazione telegrafica o telefonica vera, anche solo occasionalmente intercettata, è punito, qualora ne faccia uso o lasci che altri ne faccia uso, con la reclusione da uno a quattro anni."

Art. 617-quater, Art. 617-quinquies, Art. 617-sexies -Codice Penale

Sono il corrispondente dei 3 articoli precedenti, ma per comunicazioni informatiche o telematiche.

Tuttavia, ci sono delle caratteristiche che distinguono il reato del **617-quarter**: sono presenti, infatti, tre casi in cui si procede d'ufficio e la pena va da 1 a 5 anni.

Caso 1: se viene intercettato, interrotto o impedito il funzionamento, di un sistema utilizzato dallo Stato o da altro ente pubblico.

Caso 2: quando il fatto è compiuto da un pubblico ufficiale, con abuso dei poteri o con violazione dei doveri inerenti alla funzione o al servizio, ovvero con abuso della qualità di operatore del sistema (quel soggetto che abbia diritti o capacità tecniche specifiche relativamente a quel sistema: Amministratore del Sistema).

Caso 3: da chi esercita anche abusivamente la professione di investigatore privato.

L'Art. 617-sexies sanziona con la reclusione da 1 a 4 anni lo spoofing (alterare il proprio indirizzo IP per trarre in inganno sulla propria identità), lo spam, e tutte quelle comunicazioni che vengono alterate per poter passare eventuali filtri e per poter attribuire responsabilità a determinati soggetti.

Art. 617-septies Diffusione di riprese e registrazioni fraudolente

"Chiunque, al fine di recare danno all'altrui reputazione o immagine, diffonde con qualsiasi mezzo riprese audio o video, compiute fraudolentemente, di incontri privati o registrazioni, pur esse fraudolente, di conversazioni, anche telefoniche o telematiche, svolte in sua presenza o con la sua partecipazione, è punito con la reclusione fino a quattro anni."

La punibilità è esclusa se la diffusione delle riprese o delle registrazioni deriva in via diretta ed immediata dalla loro utilizzazione in un procedimento amministrativo o giudiziario o per l'esercizio del diritto di difesa o del diritto di cronaca."

Quindi posso registrare qualunque evento a cui partecipo, purché l'uso che ne viene fatto sia personale o giudiziario.

Art. 618 Rivelazione del contenuto di corrispondenza

"Chiunque sia venuto abusivamente a cognizione del contenuto di una corrispondenza a lui non diretta, che doveva rimanere segreta, senza giusta causa lo rivela, in tutto o in parte, è punito, se dal fatto deriva documento, con la reclusione fino a sei mesi o con la multa da euro 103 a euro 516."

Reati contro il Patrimonio

Art. 615-quater 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."

Questo articolo è il doppione informatico dell'articolo che parla della detenzione abusiva di chiavi alterate o contraffatte per le abitazioni.

È scritto male perché punisce tutti coloro che diffondono codici, password, ecc..., anche se non ha fini malevoli.

Art. 615-quinquies 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."

Anche questo articolo è scritto male perché non prevede una sanzione specifica per le alterazioni abusive, ma fa di tutta l'erba un fascio di programmi leciti e illeciti, autorizzati e non autorizzati, abusivi e non abusivi.

Gli articoli dal 635 fino al 635-quinquies presentano molti problemi e creano confusione perché, quando sono stati scritti da persone che non conoscevano abbastanza la materia, queste non si sono fatte aiutare da Informatici o esperti in materia.

Art. 635 Danneggiamento

“Chiunque distrugge, disperde, deteriora o rende, in tutto o in parte, inservibili cose mobili o immobili altrui con violenza alla persona o con minaccia, è punito con la reclusione da sei mesi a tre anni.”

Art. 635-bis Danneggiamento di informazioni, dati e programmi informatici

“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.”

Articoli scritti male e che creano confusione perché:

Puniscono maggiormente la distruzione di un sistema informatico o di un hardisk, piuttosto che la distruzione dei dati che contiene, che in realtà sono il vero patrimonio.

Art. 635-ter Danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità

“chiunque commette un fatto diretto a distruggere, deteriorare, cancellare, alterare o sopprimere informazioni, dati o programmi informatici utilizzati dallo Stato o da altro ente pubblico o ad essi pertinenti, o comunque di pubblica utilità, è punito con la reclusione da uno a quattro anni. Se dal fatto deriva la distruzione, il deterioramento, la cancellazione, l'alterazione o la soppressione delle informazioni, dei dati o dei programmi informatici, la pena è della reclusione da tre a otto 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 aumentata.”

Art. 635-quater Danneggiamento di sistemi informatici o telematici

“chiunque, mediante le condotte di cui all'articolo 635-bis, ovvero attraverso l'introduzione o la trasmissione di dati, informazioni o programmi, distrugge, danneggia, rende, in tutto o in parte, inservibili sistemi informatici o telematici altrui o ne ostacola gravemente il funzionamento è punito con la reclusione da uno a cinque 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 aumentata.”

Articoli scritti male e che creano confusione perché:

Se io prendo il monitor del PC e lo sbatto per terra, distruggendolo, mi verrà assegnata una pena di reclusione da 1 a 5 anni, pena più alta di un'eventuale distruzione di un televisore (logicamente più importante di un semplice monitor) gestita dall'Art. 635, con una pena di reclusione da sei mesi a tre anni. Qualunque sistema informatico è infatti un bene mobile, e non basta semplicemente creare articoli specifici con pena aumentata per gestire i reati informatici.

Art. 635-quinquies Danneggiamento di sistemi informatici o telematici di pubblica utilità

“Se il fatto di cui all’articolo 635-quater è diretto a distruggere, danneggiare, rendere, in tutto o in parte, inservibili sistemi informatici o telematici di pubblica utilità o ad ostacolarne gravemente il funzionamento, la pena è della reclusione da uno a quattro anni.

Se dal fatto deriva la distruzione o il danneggiamento del sistema informatico o telematico di pubblica utilità ovvero se questo è reso, in tutto o in parte, inservibile, la pena è della reclusione da tre a otto 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 aumentata.”

Questo articolo crea confusione per l’articolo 420 parla del danneggiamento a impianti di pubblica utilità, mentre il 635-quinquies parla del danneggiamento a impianti informatici di pubblica utilità. Oggi come oggi è quasi impossibile trovare un sistema che non contenga una parte informatica, quindi quale dei due articoli vanno applicati? Il 420 o il 635-quinquies?

05.05.21

Reati contro la Persona

Delitti contro la vita e l’incolumità individuale

Art. 575 Omicidio

“Chiunque cagiona la morte di un uomo è punito con la reclusione non inferiore ad anni ventuno.”

L’omicidio è possibile anche attraverso strumenti informatici come abbiamo visto precedentemente. Così com’è possibile causare lesioni e danni fisici.

Art. 595 Diffamazione

“Chiunque, comunicando con più persone, anche non contemporaneamente, offende l’altrui reputazione, è punito con la reclusione fino a un anno o con la multa fino a euro 1.032.”

L’uso degli strumenti informatici (social network), ha reso estremamente frequente il reato di diffamazione che fino a pochi anni fa era ad appannaggio esclusivo di giornalisti o personaggi pubblici importanti.

I limiti alla diffamazione sono: la **libertà di opinione**, la **libertà di pensiero**, l’esercizio del diritto alla **comunicazione** e all’**informazione**.

N.B.: solo perché una cosa è vera, non significa che non costituisca diffamazione se detta con i modi sbagliati.

Art. 599 Provocazione

“Non è punibile chi ha commesso alcuno dei fatti preveduti dall’articolo 595 nello stato d’ira determinato da un fatto ingiusto altrui, e subito dopo di esso.”

Questo vuol dire che se la diffamazione è stata fatta dopo una provocazione, mentre la persona era in uno stato d’ira dovuto ad essa, c’è una causa di non punibilità.

Dei delitti contro la libertà individuale

Art. 600-ter Pornografia minorile

“È punito con la reclusione da sei a dodici anni e con la multa da euro 24.000 a euro 240.000 chiunque:

1) utilizzando minori di anni diciotto, realizza esibizioni o spettacoli pornografici ovvero produce materiale pornografico;

2) recluta o induce minori di anni diciotto a partecipare a esibizioni o spettacoli pornografici ovvero dai suddetti spettacoli trae altri vantaggi profitti.

Alla stessa pena soggiace chi fa commercio del materiale pornografico di cui al primo comma.”

Qual è la differenza tra Pornografia, Erotismo e Arte?

Pornografico: *“Ai fini di cui al presente articolo per pornografia minorile si intende ogni rappresentazione, con qualunque mezzo, di un minore degli anni diciotto coinvolto in attività sessuali esplicite, reali o simulate, o qualunque rappresentazione degli organi sessuali di un minore di anni diciotto per scopi sessuali.”*

“Chiunque, al di fuori delle ipotesi di cui al primo e al secondo comma, con qualsiasi mezzo, anche per via telematica, distribuisce, divulga, diffonde (2) o pubblicizza il materiale pornografico di cui al primo comma, ovvero distribuisce o divulga notizie o informazioni finalizzate all'adescamento o allo sfruttamento sessuale di minori degli anni diciotto, è punito con la reclusione da uno a cinque anni e con la multa da euro 2.582 a euro 51.645.”

Tutto ciò se la detenzione e la divulgazione sono **consapevoli**.

Con **divulgazione** si intende la condivisione del materiale con un numero ampio e indefinito di soggetti.

“Chiunque, al di fuori delle ipotesi di cui ai commi primo, secondo e terzo, offre o cede ad altri, anche a titolo gratuito, il materiale pornografico di cui al primo comma, è punito con la reclusione fino a tre anni e con la multa da euro 1.549 a euro 5.164.”

La **cessione** è la condivisione del materiale con un numero predeterminato e limitato di soggetti.

Art. 600-quater Detenzione di materiale pornografico

“Chiunque, al di fuori delle ipotesi previste dall'articolo 600-ter, consapevolmente si procura o detiene materiale pornografico realizzato utilizzando minori degli anni diciotto, è punito con la reclusione fino a tre anni e con la multa non inferiore a euro 1.549.”

Ingente quantità: dipende dal contesto, può essere 20 video così come 4000.

Art. 600-quater.1 Pornografia virtuale

“quando il materiale pornografico rappresenta immagini virtuali realizzate utilizzando immagini di minori degli anni diciotto o parti di esse, ma la pena è diminuita di un terzo.

Per immagini virtuali si intendono immagini realizzate con tecniche di elaborazione grafica non associate in tutto o in parte a situazioni reali, la cui qualità di rappresentazione fa apparire come vere situazioni non reali.”

Fotomontaggi per creare immagini virtuali di minori in pose sessualmente esplicite. Sono rari perché i pedofili vogliono immagini vere.

Delitti contro l'eguaglianza

Art. 604-bis Propaganda e istigazione a delinquere per motivi di discriminazione razziale etnica e religiosa

“Salvo che il fatto costituisca più grave reato, è punito:

a) con la reclusione fino ad un anno e sei mesi o con la multa fino a 6.000 euro chi propaganda idee fondate sulla superiorità o sull'odio razziale o etnico, ovvero istiga a commettere o commette atti di discriminazione per motivi razziali, etnici, nazionali o religiosi;

b) con la reclusione da sei mesi a quattro anni chi, in qualsiasi modo, istiga a commettere o commette violenza o atti di provocazione alla violenza per motivi razziali, etnici, nazionali o religiosi.”

Viene punita l'**istigazione**: attività con cui un soggetto spinge o convince un altro soggetto a commettere un reato. Si avvicina molto al reato d'**opinione personale**, è quindi fondamentale saperle distinguere.
Es.: Opinione Personale: "Le tasse dovrebbero essere abbassate perché la maggior parte dei cittadini non riesce a pagarle."

Istigazione: "Le tasse sono troppo alte, smettete tutti di pagarle."

Anche qui è bene stare attenti a come ci si esprime, soprattutto sui social.

Art. 609-bis Violenza sessuale

"Chiunque, con violenza o minaccia o mediante abuso di autorità, costringe taluno a compiere o subire atti sessuali è punito con la reclusione da sei a dodici anni."

Violenza: può essere sia fisica che morale.

Minaccia: deve essere credibile, riguardare un danno ingiusto alla persona o ai suoi beni, oppure deve essere fatta mediante l'abuso di autorità.

La violenza sessuale è un reato che può essere commesso in via informatica e a distanza: inviare foto hard a un minore, costringere un minore a compiere atti sessuali su di sé, ecc...

Una violenza sessuale è tutto ciò che lede la libertà sessuale dell'individuo. Tutti quegli atti non desiderati che coinvolgono le zone erogene (anche la bocca, ad es., con un bacio), costituiscono violenza sessuale.

"Alla stessa pena soggiace chi induce taluno a compiere o subire atti sessuali:

- 1) *abusando delle condizioni di inferiorità fisica o psichica della persona offesa al momento del fatto;*
- 2) *traendo in inganno la persona offesa per essersi il colpevole sostituito ad altra persona."*

Il reato di violenza sessuale si applica a tutti coloro che simulano, fingono una professione, uno status, per ottenere un vantaggio sessuale. (es.: il falso ginecologo)

Anche quando il soggetto durante una videochat erotica si sostituisca ad un altro soggetto e convince l'interlocutore a compiere atti sessuali. (es.: l'uomo adulto che si finge un ragazzino per indurre l'interlocutore minorenne a inviare materiale pornografico)

Art. 609-quater Atti sessuali con minorenne

Prevede che si applichi la stessa pena della violenza sessuale a chi compie atti sessuali con un soggetto che non ha compiuto ancora i **14 anni**, l'età del consenso al compimento di atti sessuali (autodeterminazione).

Art. 609-sexies Ignoranza dell'età della persona offesa

Nessuno può invocare a sua discolpa l'ignoranza dell'età della persona offesa.

Art. 609-octies Violenza sessuale di gruppo

È stato stabilito che partecipa alla violenza sessuale di gruppo anche colui che si limita a filmare i compagni che compiono la violenza sessuale.

Art. 609-unidcies Adescamento di minorenni

"Chiunque, allo scopo di commettere i reati di cui agli articoli 600, 600-bis, 600-ter e 600-quater, anche se relativi al materiale pornografico di cui all'articolo 600-quater.1, 600-quinquies, 609-bis, 609-quater, 609-quinquies e 609-octies, adesca un minore di anni sedici, è punito, se il fatto non costituisce più grave reato, con la reclusione da uno a tre anni. Per adescamento si intende qualsiasi atto volto a carpire la fiducia del minore attraverso artifici, lusinghe o minacce posti in essere anche mediante l'utilizzo della rete internet o di altre reti o mezzi di comunicazione."

Art. 612-bis Atti persecutori

Riguardano la condotta del soggetto che perseguita con attività particolari, un altro soggetto (attraverso l'invio di messaggi, attraverso la presenza, ecc...), può essere commesso sia fisicamente che a livello informatico.

Art. 612-ter Diffusione illecita di immagini o video sessualmente espliciti (Revenge Porn)

Diffusione senza il consenso delle persone interessate, con pena di reclusione da 1 a 6 anni. Si applica anche a coloro che ricevono il video e continuano a ri-condividerlo.

Come L'informatica impatta sul Diritto

17.05.21

- **Processo Civile Telematico (PCT):** è un'applicazione diretta di tecnologie informatiche al mondo del processo. È una procedura che consente all'avvocato di gestire, affrontare e organizzare un processo sulla base di una piattaforma informatica, a livello nazionale, in modo tale da consentire di depositare prove e atti, interfacciarsi con il giudice, senza il bisogno di recarsi in segreteria.
- **Tool di Analisi Forense:** programmi di uso comune a chi fa Informatica Forense, che consentono di affrontare un caso.
- **Software Gestionali** per lo studio legale
- **Virtualizzazione degli esperimenti giudiziali** (introdotto dall'informatica): il codice di procedura penale stabilisce che, se necessario, il giudice può disporre la ricostruzione per quanto possibile del fatto storico alla base del delitto (esperimento giudiziale). Questa è un'attività finalizzata a ricreare nella nell'aula di giustizia quanto avvenuto in ambito di scena del crimine, per capire se tutto quello che è stato raccontato, detto e prodotto, è compatibile con la realtà.

C'è un problema di fondo perché il Codice Penale stabilisce che l'esperimento giudiziale deve essere, per quanto possibile, conforme allo svolgimento dei fatti. Questo "simile" è stato interpretato per molti anni in maniera molto ampia.

Ecco perché la virtualizzazione è diventata di fondamentale importanza, così da ricostruire nel migliore dei modi la scena del crimine.

La prima cosa che deve essere fatta è renderizzare nel modo più preciso possibile la scena del crimine, la seconda è quella di avere degli standard documentati da una serie di manuali operativi che tutte le forze dell'ordine del mondo utilizzano (es.: la macchina fotografica, il sistema di rivelazione delle misure degli ambienti, ecc.).

Il criminologo informatico forense, ha il compito di creare una scena virtuale che consenta agli investigatori di avere un panorama completo della scena del crimine, di evidenziare eventuali tracce, di prendere misure, riferimenti, e fare prospetti, nel modo più preciso possibile così da ridurre al minimo il margine d'errore. È possibile simulare anche reati digitali (es.: DOS).

Molto utile per la didattica e per permettere a studenti di lavorare su simulazioni.

- **Processi:** che consentono all'investigatore di elaborare identikit virtuali (processi di aging). Questi software devono reggere in tribunale, quindi devono essere scientificamente provati.

Il riciclaggio informatico presenta delle caratteristiche particolari rispetto a quello classico.

Art. 648 Ricettazione

Reato di un soggetto che non ha partecipato al reato principale (furto ad es.), ma al fine di procurare a sé o ad altri un profitto, acquista, riceve od occulta denaro o cose provenienti da un qualsiasi delitto, o comunque si intromette nel farle acquistare, ricevere od occultare.

La ricettazione e il riciclaggio vengono puniti in maniera più grave rispetto al reato base perché incentivano i soggetti che compiono il delitto a perseguire la loro condotta criminosa, dato che permettono loro di monetizzare sull'oggetto del furto e di sottrarsi alle indagini.

Art. 648-bis Riciclaggio

Mentre la ricettazione viene svolta generalmente convertendo il bene del reato in un altro bene (tipicamente in denaro), nel riciclaggio abbiamo una serie di attività volte a ripulire il denaro sporco in modo tale da farlo apparire pulito e farlo reimmettere nel circuito economico.

Si compone di **3 fasi**:

- 1) **Placement:** immettere il denaro sporco nel circuito bancario. È la fase più pericolosa.
- 2) **Lavaggio:** il denaro viene ripulito reinvestendolo nel circuito finanziario e cercando di nascondere il più possibile le sue origini. (es.: casinò)
- 3) **Integration:** il denaro riciclato viene reimmesso nel circuito finanziario legittimo, tipicamente tramite investimenti apparentemente legittimi. È in questa fase che il denaro cattivo caccia quello buono, perché gli investitori illegittimi sono disposti a strapagare per ottenere determinati beni o iniziare determinate attività, piuttosto che lasciare marcire i soldi non sapendo come reimmetterli nel sistema economico legittimo. Questo porta ad un conseguente aumento dei prezzi vertiginoso per quelle attività, che gli imprenditori legittimi non possono permettersi di pagare.

Il **cyberriciclaggio** è molto più difficile da combattere rispetto a quello classico perché il flusso dei bit delle transazioni elettroniche è più difficile da seguire.

Abbiamo due tipi di cyberriciclaggio:

1. Riciclaggio Digitale **Integrale:** taglio fuori tutti gli intermediari e il denaro viene immediatamente digitalizzato (es. pagamento diretto in bitcoin).
2. Riciclaggio Digitale **Strumentale:** l'informatica è usata come mero strumento. Per la fase di placement, generalmente pericolosa, è un grande upgrade.

Con reati informatici intendiamo tutti i reati che hanno in qualche modo riguardato un computer. Quando parliamo di Informatica Forense non parliamo solo dell'analisi dei dispositivi elettronici, ma dell'analisi di qualsiasi tipologia di informazione che viaggi attraverso un dispositivo elettronico. Abbiamo quindi:

- Analisi dei **dispositivi fisici**
- Analisi dei **dispositivi virtuali** (macchina virtuale, cloud)
- Analisi dell'**informazione** che viaggia in rete

In generale si tende a distinguere:

1. **Computer Forensics**: quella che riguarda i tablet, i laptop e i desktop.
2. **Mobile Forensics**: dispositivi mobile come i classici smartphone.
3. **Network Forensics**: analisi del traffico della rete.
4. **Cloud Forensics**: analisi dei dati contenuti in un Cloud.
5. **Blockchain Forensics** analisi della Blockchain e delle interazioni tra i vari utenti che hanno partecipato agli scambi della Blockchain.

Tutte queste aree hanno software, dispositivi e procedure differenti d'analisi. Questo perché la **modalità d'approccio** al problema dipende dal **target** dell'analisi (non posso approcciare un cellulare come approccio un computer desktop).

Quando dobbiamo fare un'analisi forense dobbiamo chiederci: perché stiamo facendo questa analisi? Perché a seconda dell'obiettivo, potremmo trovarci a dover operare in modalità differenti.

Art. 359 Accertamenti Tecnici -Codice Penale (ripetibili)

Art. 360 Accertamenti Tecnici Irripetibili -Codice Penale

Il concetto di **irripetibilità** è legato alla natura intrinseca dei dati che andiamo ad analizzare: tutti gli accertamenti sono ripetibili e irripetibili. Questo perché niente è uguale nel tempo e tutto muta. Quindi ogni volta che ripeto l'accertamento avrò sotto esame un oggetto differente.

Accertamenti ripetibili: quegli accertamenti dove l'oggetto esaminato non subisce rilevanti variazioni dal punto di vista investigativo, nell'esecuzione dell'analisi. Per esempio: scattare fotografie alla scena del delitto non muta lo stato dei luoghi.

Accertamenti non ripetibili: tutti quelli che hanno ad oggetto dei dati soggetti a mutamento. Per esempio: l'autopsia, acquisizione dei dati di una rete o di un cloud.

L'immutabilità dal punto di vista investigativo di un oggetto o di una persona o di uno status, è legata sia al contenuto e alle **caratteristiche tecniche** di quell'oggetto, sia ad altri elementi esterni come il **trascorrere del tempo**.

Per proteggere i dati abbiamo il **sequestro**, così da impedire che il soggetto commetta ulteriori reati e alteri le prove. A seconda della natura del sequestro, cambiano anche le modalità in cui può essere fatto.

Nel sequestro cautelare, il dispositivo può essere trattenuto per sempre, mentre in quello probatorio, una volta acquisita l'immagine dei dati, deve essere restituito.

Sequestro Probatorio

Finalizzato ad **acquisire le prove**. Il problema è che, nel momento in cui si sequestra un computer, si vanno a sequestrare anche altri dati che non sono collegati con il reato.

Il sequestro probatorio può essere finalizzato come **attività esplorativa** ovvero, quando sono stati acquisiti tutti i dati di un computer sotto sequestro, la controparte può chiedere di accedere a tali dati. Così facendo però, non accede solo ai dati relativi al presunto reato, ma a *tutti* i dati del computer, cosa che ovviamente può causare dei grandi problemi ai proprietari della macchina.

Quindi si è deciso di procedere in questo modo: copiare tutti i dati del PC su un hardisk e sigillare tale hardisk in una busta, così che non possa essere manomesso. Dopodiché vengono acquisiti, attraverso la ricerca tramite keyword, solo i dati relativi al procedimento penale in corso.

Come si procede a garantire la **ripetibilità dell'accertamento**? La procedura di acquisizione dei beni varia a seconda del target:

- **Computer:** si estraе fisicamente l'hard disk dal dispositivo e lo si collega ad un dispositivo hardware con 2 porte, una solo per la lettura e protetta da scrittura, e l'altra che può leggere e scrivere. Viene fatta la copia dell'hash di quel dispositivo così da controllare, una volta completata la copia, che l'hash sia rimasto invariato; oppure si può fare lo stesso prendendo una copia dell'immagine del dispositivo e poi controllando l'hash dell'immagine. Poi l'hardisk viene collegato in modalità di sola lettura in modo da essere sicuri al 100% che quel dispositivo non venga modificato, e viene acquisito nel dispositivo di destinazione che diventa "**target device**", cioè dispositivo di copia. Una volta acquisita la copia si controlla l'hash.

Posso **acquisire i dati** in 3 modalità:

- **Copia raw:** copio settore per settore tutto il contenuto del dispositivo nel dispositivo target, così da avere alla fine due dispositivi identici.
- **Copia compressa:** ormai i dispositivi informatici hanno hardisk sempre più capienti, ed è diventato anti-economico effettuare le copie raw. Con le copie compresse si prendono i dati dell'hardisk originale e vengono messi in un file zip. In questo modo non ho un'immagine speculare dei due hardisk, ma un hardisk normale e funzionante, e un'immagine di quell'hardisk, un file endocontenuto (contenuto in un pacchetto) che non può essere modificato dall'utente perché ha un determinato hash.
- **Selezione dei dati** da copia compressa: seleziono dal file compresso solamente i dati relativi al reato e creo un nuovo pacchetto, che verrà sottoscritto digitalmente dai consulenti (viene preso l'hash) e analizzato da tutte le parti singolarmente.

Una volta che abbiamo il pacchetto dei dati, ognuno lo analizza come meglio crede perché tanto ormai i dati sono cristallizzati. Esistono vari **tool** per analizzare i dati che si dividono in due grandi categorie: open source, proprietari. Nel momento che io confermo che l'accertamento è ripetibile posso utilizzare quello che preferisco, così in caso di risultati differenti è possibile un confronto.

10.05.21

Attori dei Crimini Informatici

- Vittima
- Criminale
- Polizia Giudiziaria, Polizia Postale e delle Comunicazioni, Questura, Guardia di Finanza, Carabinieri, Polizia Locale
- Magistratura
- Avvocati
- Media
- Web
- ISP (Internet Service Providers): forniscono informazioni su chi e come ha commesso il reato.
- Consulenti tecnici

Scene del Crimine

1. Scene del crimine **Statiche**: ad esempio le chiavette USB.
2. Scene del crimine **Dinamiche**: ad esempio un computer acceso, perché la scena del crimine non è congelata. Il computer mentre rimane acceso continua a scaricare e inviare file, quindi cambia continuamente. Bisogna congelare la scena del crimine il prima possibile.

Reati

- Reati **Storici**: pedopornografia, Hacking, Truffe, Sostituzione di persona, ecc...
- **Nuovi Reati**: Romatic scam, Man in The Middle, Sex Extortion, Cyberterrorism.

Time Line di un'Indagine

1. Acquisizione della notizia di reato: può avvenire in vari modi, ad esempio per denuncia, per reato d'ufficio (quando le forze dell'ordine vedono effettivamente il crimine che si sta svolgendo), ecc... Quindi so che è successo qualcosa a scapito di qualcuno.
2. Definizione della procedibilità: posso investigare su questa cosa? Serve la querela per investigare oppure no?
3. Definizione obiettivi investigative: dove voglio arrivare? Se devo solo denunciare una persona farò determinati atti, se invece voglio mandarla in carcere ne farò altri, avendo un piano investigativo ad esempio.
4. Definizione Piano Investigativo
5. Raccolta delle fonti di prova:
 - a. fonte di prova: non è ancora tecnicamente una prova, perché una prova si forma durante il processo.
 - b. Prova: oggetto che è in grado di provare un fatto. Possono essere o preconstituite, cioè preesistenti al procedimento, oppure costituite durante il giudizio.
 - c. Mezzi di ricerca della prova
6. Revisione dell'indagine: ho fatto tutto quello che potevo fare? Revisiono l'indagine dall'inizio. Se è tutto a posto, procedo.
7. Report finale (Informativa finale): dico al PM il risultato della mia indagine.

Modalità d'Indagine (Raccolta delle fonti di prova)

- **Diretta**: perquisizioni, sequestri, intercettazioni, ecc...
- **Indiretta**: sommarie informazioni, spontanee, ecc...

Strumenti del Mestiere

- Computer
- Strumenti specifici: ufed, encase, ecc...
- Software: ad es. Encase.
- Fattore C: fortuna.

Reati

- **Pedopornografia**
- **Truffe On Line:**

Art. 640 Truffa (normale)

“Chiunque, con artifizi o raggiri, inducendo taluno in errore, procura a sé o ad altri un ingiusto profitto con altrui danno, è punito con la reclusione da sei mesi a tre anni e con la multa da euro 51 a euro 1.032.”

Art. 640-ter Frode informatica

“Chiunque, alterando in qualsiasi modo il funzionamento di un sistema informatico o telematico o intervenendo senza diritto con qualsiasi modalità su dati, informazioni o programmi contenuti in un sistema informatico o telematico o ad esso pertinenti, procura a sé o ad altri un ingiusto profitto con altrui danno, è punito con la reclusione da sei mesi a tre anni e con la multa da euro 51 a euro 1.032.”

- **Hacking:** processo di bypassare le protezioni di un computer al fine di accedervi, per finalità legali o illegali. Art. 615 Ter Accesso abusivo ad un sistema informatico o telematico.
- **Cracking:** processo di bypassare le protezioni di un computer al fine di accedervi, per finalità puramente criminali. Gli Hacker creano, mentre i cracker distruggono. In particolare i cracker praticano attività illegali come rubare i numeri delle carte di credito, diffondere virus, distruggere file, o raccogliere dati personali da rivendere.
- **Atti Persecutori:**

Art. 612-bis Atti Persecutori

“chiunque, con condotte reiterate, minaccia o molesta taluno in modo da cagionare un perdurante e grave stato di ansia o di paura ovvero da ingenerare un fondato timore per l'incolumità propria o di un prossimo congiunto o di persona al medesimo legata da relazione affettiva ovvero da costringere lo stesso ad alterare le proprie abitudini di vita.

La pena è aumentata se il fatto è commesso dal coniuge, anche separato o divorziato, o da persona che è o è stata legata da relazione affettiva alla persona offesa ovvero se il fatto è commesso attraverso strumenti informatici o telematici.”

Stato d'ansia: o avendo un certificato del medico (pronto soccorso ad es.), o l'ufficiale di polizia giudiziaria da atto che la persona è in uno stato d'ansia e di alterazione, quando questa va a fare la denuncia.

- **Diffamazione**
- **Sostituzione di persona**

Art. 494 Sostituzione di Persona

“Chiunque, al fine di procurare a sé o ad altri un vantaggio o di recare ad altri un danno, induce taluno in errore, sostituendo illegittimamente la propria all'altrui persona, o attribuendo a sé o ad altri un falso nome, o un falso stato, ovvero una qualità a cui la legge attribuisce effetti giuridici, è punito, se il fatto non costituisce un altro delitto contro la fede pubblica con la reclusione fino a un anno.”

- **Romantic Scam:** generalmente rivolta verso le donne. Uomini che adescano donne online, fingendosi militari Americani, che si trovano in luoghi con problemi di comunicazione, e che coltivano la relazione per mesi per poi chiedergli ingenti somme di denaro.

Mentre con gli uomini succede che vengano adescati da donne che gli chiedono di spogliarsi in videochiamata, registrandoli di nascosto, e poi ricattandoli di diffondere il filmato a tutti i loro amici di facebook se non pagano una determinata cifra. In questo ultimo caso la soluzione è di cancellare immediatamente il profilo facebook e non riaprirlo più.

- **Revenge Porn**
- **Cyberterrorismo:** utilizzo del cyberspazio (Internet) per fini terroristici, ovvero, diffondere la paura e il panico nella popolazione destabilizzando l'ordine e la sicurezza pubblica, per ragioni politiche, ideologiche o religiose. Si manifesta con due attività prevalenti: propaganda e attività diretta (utilizzare direttamente il cyberspazio come mezzo per colpire e dare dimostrazione della propria potenza di fuoco. Partendo da attacchi dimostrativi come il defacement di un sito web, sino alla vera e propria intrusione in un sistema informatico anche complesso. I principali obiettivi di questa attività sono generalmente le infrastrutture critiche di un paese, non solo per creare malfunzionamenti e diffondere il panico tra la popolazione, ma anche per poter sottrarre informazioni segrete). Si divide in interno (Brigate Rosse), e esterno (Al Quaeda).
- **Cyberwarfare:** è l'insieme delle attività di preparazione e conduzione delle operazioni militari eseguite nel rispetto dei principi bellici condizionati dall'informazione. Si può tradurre nell'intercettazione, nell'alterazione e nella distruzione dell'informazione e dei sistemi di comunicazione nemici, procedendo a far sì che sul proprio fronte si mantenga un relativo equilibrio dell'informazione. La guerra cibernetica si caratterizza per l'uso di tecnologie elettroniche, informatiche e dei sistemi di telecomunicazione.

Indagine su Profili Facebook

- **Accertamenti PG:** dopo aver raccolto tutti gli elementi della denuncia, si dovrà chiedere alla società Facebook, sul portale dedicato facebook.com/records, i dati di cui si necessita (con apposito decreto) indicando l'ufficio richiedente al quale potrà essere reindirizzata una risposta via mail.
- **Procedure di Emergenza:** in caso di segnalazioni di tentativi di suicidio o altra situazione dove vi sia un pericolo immediato, si dovrà attivare la procedura di emergenza tramite l'apposito portale facebook.com/records, al fine di scoprire l'indirizzo IP di chi sta tentando di suicidarsi.