COS'E'L'ANONIMATO

Sinteticamente. – Quando si parla di anonimato si possono toccare diversi ambiti del diritto.

--- > nel diritto civile: si parla di anonimato in riferimento al diritto d'autore – alla protezione dei dati personali – all'anonimato di una madre o di un padre …

--- > nel diritto penale: si fa riferimento all' anonimato quando si parla di aggravanti in caso di reati che riguardano minacce …

--- > nel diritto processuale penalistico: si parla di anonimato in riferimento a notizie anonime di reato

--- > nel diritto amministrativo: si parla di anonimato in riferimento ai concorsi pubblici

--- > nel diritto costituzionale: si parla di anonimato in riferimento al diritto di manifestazione del pensiero[1]

In questo nostro contesto interessa analizzare l'anonimato con riferimento alla rete ed ai dati personali.

DEFINIZIONE: IL RN normativo che offre la definizione di anonimato nel modo più articolato è il testo del Codice della Privacy (d.lgs. n. 196 del 2003) art. 4, comma 1 lett. n) --- > il quale così definisce il dato anonimo: "*n*) «dato anonimo», il dato che in origine, o a seguito di trattamento, non può essere associato ad un interessato identificato o identificabile;"

Nel Codice Privacy si parla dunque di anonimato in riferimento al c.d. "dato".

DATO

Per dato si intende il dato personale ossia riferito ad una determinata persona. Dal legislatore europeo viene definito come "informazione personale"[2].

Esiste, nelle definizioni del Codice Privacy, la definizione Dato Anonimo. Ma in realtà questo non ha niente a che vedere con l'Anonimato che si affronta in questo contesto --- > Il dato anonimo, per il Codice è quello contrapposto al dato personale ossia: il dato che in origine, o a seguito di trattamento, non può essere associato ad un interessato identificato o identificabile. **Ossia un dato comune o generico.**

Ulteriori chiarimenti sul Dato sono contenuti nella lezione che tratta della **Privacy in genere (vedere).**

[1] G. Finocchiaro (a cura di), Diritto all'anonimato. Anonimato, nome e identità personale.
[2] Per la prima volta nella risoluzione europea del Consiglio d'Europa n. 22 del 1973. Concetto più volte ripreso in seguito da altre Risoluzioni fino ad essere ribadito nella Convenzione di Strasburgo per la protezione delle persone in relazione al trattamento dati, del 28 gennaio 1981 (art. 2, co. 1).

ANONIMATO IN INTERNET

Quando si parla di anonimato in rete c'è sempre una profonda frattura tra chi appoggia il diritto di anonimato in Rete (=non presentarsi con una propria identità) e chi, al contrario, sostiene che non si può diffamare qualcuno senza essere poi rintracciabile.

Il problema sorge in quanto l'ambiente internet permette una diffusione virale delle informazioni che sono, di fatto, in grado di rimbalzare senza controllo di blog in blog o su i vari social network. In un simile contesto una notizia falsa o diffamatoria è in grado di procurare grossi danni.

È difficile, dunque, per chiunque prendere una posizione equa sul fenomeno.

Il diritto può venire incontro a questa esigenza.

Tipi di anonimato

L'anonimato può essere svolto in ambito

- (Privato) Blog-Forum-Chat --- > In questo caso è espressione di Libertà del Pensiero
- (Privato) NELLE TRANSAZIONI COMMERCIALI ad esempio nel commercio elettronico. In questa ipotesi può dare origine ad eventi dannosi quali: Furto d'identita' nel FISHING, SPAMMING, FRODI INFORMATICHE --- > perciò è considerato illecito.

Alcuni casi che fanno riflettere:

1. A favore dell'anonimato si potrebbero portare casi come quelli pubblicati ad esempio, su Il Sole24ore che in un articolo di qualche tempo fa ha ricordato il ruolo importante svolto dalla rete in merito ai fatti di Teheran, "dove garantire l'anonimato di chi informava il mondo tramite Twitter di quanto accadeva per le strade della capitale iraniana era una questione di vita o di morte" e di quanto sia stato determinante e provvidenziale il fattore dell'anonimato in questo caso.
2. A sfavore dell'anonimato fra i tanti episodi si può ricordare il caso "di voli gratuiti offerti dalle compagnie aeree americane per personale medico che fosse pronto a partire per Haiti" durante la tragedia che colpì il territorio. Notizia che poi si rivelò una bufala perché falsa.
3. Cosa dire poi del caso wikileaks che si pone al centro dell'amletica scelta. Ha ragione Assange a pubblicare i documenti delle varie diplomazie degli Stati di tutto il mondo, scoprendo giochi di potere sconosciuti ai più e creando così una informazione libera e trasparente al servizio del

cittadino? Oppure ha torto perché così facendo viola segreti di Stato inquietanti ma anche delicati per l'equilibrio diplomatico fra le varie potenze mondiali?

Una soluzione potrebbe consistere nel garantire un filtro, da parte dei responsabili dei servizi di diffusione online, delle notizie, compresi i social network. Ma la soluzione non è affatto così semplice perché non si sa se questo sia effettivamente possibile a causa della enorme mole di lavoro che ci sarebbe e della precarietà della scelta di decidere cosa sia lecito far passare dal filtro perché questa scelta verrebbe effettuata in modo decisamente soggettivo.

Conseguenze preoccupanti potrebbero essere più complicate del male che si tenta di correggere, come ad esempio il pericolo di cadere nella censura oppure quello di snaturare la comunicazione in rete della sua principale caratteristica che la rende invincibile, ossia la sua immediatezza intesa sia come comunicazione effettuata in tempo reale sia come comunicazione che non viene mediata da alcuno.

COSA DICE IL DIRITTO

La legge "dice" che c'è una **contrazione** del diritto all'anonimato difronte ad altri diritti prevalenti.

Ma se la formula è chiara, non lo è la sostanza, perché non è affatto facile stabilire quali sono questi diritti prevalenti e quando possono prevalere sul diritto all'anonimato.

1. Esempio più volte citato è quello della **diffamazione on line** dinanzi alla quale il diritto all'anonimato, anche qualora sia connesso con il diritto di libera manifestazione di pensiero o di diritto alla protezione di dati personali, **soccombe** di fronte al diritto al rispetto dell'onore o della reputazione altrui.
2. Esempio **dell'attacco a siti web** con danno e loro momentanea inutilizzabilità (una pratica a volte effettuata per sfida, o per provocazione o ancora per contestazione politica --- > c.d. danneggiamento da *defacement* o da *Ddos attack o netstrike*). Anche in questi casi si è ormai sempre più orientati **a sacrificare** il diritto all'anonimato rispetto alla funzione svolta da questi canali.
3. Esempio di accesso abusivo a sistema informatico. In questi casi il diritto all'anonimato **non può essere invocato**.
4. Esempio di furto di identità --- > in questo caso la **tutela alla propria identità personale ha il sopravvento** su qualsiasi forma di anonimato da parte del danneggiante.

Sostanzialmente si può affermare che l’anonimato in internet non può essere tutelato laddove ci sia la necessità di identificare gli autori di condotte ingiuste e pregiudizievoli rispetto a diritti altrui.

Si può dire che l’anonimato in rete è ben tollerato dal diritto, tanto da essere riconosciuto come la “normalità” dell’attività dell’utente in rete. Ma subisce forti limitazioni in presenza di realizzazione di attività criminose.

L’ANONIMATO RELATIVO

Occorre chiarire che più che Anonimato puro il diritto accetta un Anonimato che potrebbe essere definito “relativo”. Lo dimostra tutto cio’ che si è detto sino ad ora.

L’Anonimato relativo è quell’Anonimato che riconosce a ciascuno il diritto di navigare in Rete indossando una specie di maschera solo dopo aver consegnato agli intermediari della comunicazione la propria reale identità. Una sorta di anonimato protetto che indirettamente conferma il principio dell'identificabilità (in non giuridichese: puoi agire anche in forma anonima = ossia non in chiaro, ma devi essere rintracciabile = ossia identificabile in caso di necessità).

Su di una cosa la legge non ammette deroghe ed è chiara. Sulla figura del Provider. Unici soggetti a cui l’anonimato non è concesso. A questi soggetti è preclusa la possibilità di nascondersi, celarsi o dissimulare la propria reale identità essendo loro espressamente richiesto di presentarsi e registrarsi in appositi albi ed elenchi tenuti da diverse Pubbliche Autorità.

Sulla figura del Provider e sulle sue funzioni e responsabilità si rinvia alla lezione sul **Commercio Elettronico** (**vedere**).

Sostanzialmente nel confronto fra :

Diritto di riservatezza < --- > Libertà di espressione (Anonimato) < --- > Prevenzione del crimine

Prevale la prevenzione del crimine.

IL QUADRO NORMATIVO

Il quadro normativo che disciplina e riduce il diritto all’anonimato in rete è rappresentato dalle norme che si rifanno alla **Sicurezza Informatica (vedere lezione)** a cui si rinvia. In sintesi i testi normativi di base sono:

--- > Codice sulla Privacy

Nell'allegato B del Codice della privacy il punto 10 del Disciplinare Tecnico più volte detta regole volte a proteggere la riservatezza del legittimo utente, ma tende anche a definire la tracciabilita' del dato. La legge, sostanzialmente, vuole conoscere in ogni momento chi e perche' ha utilizzato quella determinata macchina.

--- > pacchetto Pisanu (*)

Sul pacchetto Pisanu ci sono stati in questo ultimo periodo interventi caotici e poco chiari --- > vedere lezione su Sicurezza Informatica.

--- > Direttiva 2006/24/CE

Il caso pratico. Diritto all'anonimato vs Diritto d'autore. Il caso Peppermint

Un caso complicato, per le implicazioni ulteriori che si sono avute, è quello denominato "**caso Peppermint"**.

Può accadere che il diritto all'anonimato (inteso come tutela dei propri dati personali) prevalga nei confronti di diritti patrimoniali come, ad esempio, in caso di conflitto con (l'aspetto patrimoniale legato al) Diritto d'autore (o meglio alla proprietà intellettuale). È questo il caso Peppermint.

… prima le parti interessate …

Sul caso Peppermint si espresse Tribunale di Roma, ord., 16 luglio 2007 (vedere Casi di studio: Tribunale Roma, ord., 16 luglio 2007, causa Peppermint e Techland vs Telecom)

La Peppermint, casa discografica, titolare del diritto d'autore violato, richiede all'ISP Telecom, di esibire i dati anagrafici di alcuni intestatari di linee telefoniche che, connettendosi a reti P2P, **avrebbero** condiviso *file* di opere tutelate in violazione del diritto di cui all'art. 16, L. 633/1941.

In questa decisione del giudice viene capovolta una prassi che si era assodata con il tempo (cfr. precedenti sentenze opposte: Tribunale di Roma in data 19 agosto 2006, 22 settembre 2006 e 9 febbraio 2007. Anche un caso molto simile - il caso FAPAV vedi Casi di studio- è stato risolto con una sentenza opposta che sostanzialmente nega la natura di dato personale all'IP e dunque non lo tutela all'interno della privacy --- > tribunale Roma 15 aprile 2010), in quanto il Tribunale di Roma, sezione specializzata in materia di proprietà industriale ed intellettuale, ha rigettato il ricorso presentato dalla Peppermint volto ad ottenere l'esibizione da parte dalla Wind Telecomunicazioni S.p.a. dei dati anagrafici necessari all'identificazione di (presunti) responsabili di violazioni del diritto d'autore di cui le stesse sono titolari. Sostanzialmente il giudice ha

considerato legittimo il rifiuto dell'ISP convenuto di rendere alla Peppermint i dati di identificazione (personali) di alcuni utenti che la Peppermint **dubitava** si fossero scambiati file musicali protetti dal diritto d'autore.

Nel caso si innestò un discorso parallelo ed altrettanto importante, in quanto risultò che la Peppermint si avvalse del lavoro di una società specializzata in informatica (svizzera, la Logistep, utilizzata anche dalla società Techland con riferimento a software relativi a giochi) per monitorare sistematicamente le reti *Peer to Peer* tramite l'utilizzo di software specifici e "spiare" così gli utenti. In realtà grazie a questi software utilizzati, le società avevano individuato numerosi indirizzi IP (che identificarono i computer collegati ad Internet) relativi a utenti **ritenuti responsabili** dello scambio illegale di file, risalendo così ai nomi degli utenti, anche italiani, al fine di potere ottenere un risarcimento del danno.

… poi il Garante …

Per questo motivo anche il Garante della privacy si costituì in giudizio presso il Tribunale di Roma nelle cause intentate dalla Peppermint nei confronti di gestori telefonici con l'intento di verificare se nella vicenda fossero stati rispettati tutti i diritti di protezione dei dati personali

Ebbene il Garante affermò giustamente che le società private non possono svolgere attività di monitoraggio sistematico per individuare gli utenti che si scambiano file musicali o giochi su Internet, ritenendo illecita, a sua volta, l'attività svolta da tali società.

Nella sua motivazione viene affermato che: a) la direttiva europea sulle comunicazioni elettroniche vieta ai privati di poter effettuare monitoraggi[3]; b) "non sono stati rispettati i principi di trasparenza e correttezza, perché i dati sono stati raccolti ad insaputa sia degli interessati sia di abbonati che non erano necessariamente coinvolti nello scambio di file"; c) l'obbligo delle società che hanno effettuato il monitoraggio di cancellare i dati personali degli utenti che hanno scambiato file musicali e giochi attraverso il sistema P2P.

… e poi anche l'ADICONSUM …

Ma il caso Peppermint non si è fermato qui. Ha continuato ad evolversi, tant'è che l'Adiconsum (l'associazione a tutela dei consumatori) è entrata nel caso costituendosi in tutti i procedimenti intrapresi innanzi ai giudici italiani dalla casa discografica Peppermint Jam Records, con l'intento di far dichiarare, ai giudici aditi, la prevalenza del diritto alla privacy sul diritto di sfruttamento economico dell'opera intellettuale" oltre al riconoscimento di una illegittimità dei metodi utilizzati dalla Peppermint per la ricerca dei singoli indirizzi IP dei vari utenti.

ANONIMATO E IDENTIFICAZIONE

[3] Trattamenti di dati massivi, capillari e prolungati nei riguardi di un numero elevato di soggetti

È bene ricordare che in rete è possibile lavorare identificandosi come utente attraverso un indirizzo IP.

Pertanto "un messaggio reso in forma anonima, ossia non "firmato" (nel senso: "privo dell'indicazione del nome e del cognome dell'autore"), non implica l'impossibilità di identificazione del soggetto che l'ha inviato. Infatti, tecnicamente, è possibile risalire all'**indirizzo IP** del soggetto che ha inviato il messaggio eventualmente diffamatorio e, tramite l'**Internet Service Provider**, risalire all'identità del soggetto a cui l'IP è stato assegnato, sia esso un IP statico o dinamico".

IP =DATO PERSONALE?

Tutto questo disquisire parte da una domanda, se cioè l'IP possa essere trattato oppure no come un dato personale.

Non c'è unanimità in merito.

Brevemente si riassumono gli aspetti salienti del problema:

Per il diritto: l'art. 4 d.lgs. 196/2003 (T.U. dati personali) cosi' recita: *b) "dato personale", qualunque informazione relativa a persona fisica, persona giuridica, ente od associazione, identificati o identificabili, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale*.

Questo significa che l'IP può considerarsi dato personale solamente quando il "titolare del trattamento" possa collegarlo a qualche altro dato che consenta una identificazione univoca del soggetto giuridico al quale tale indirizzo si riferisce.

L'IP potrebbe essere paragonato alla targa di una macchina come tale è in grado di identificarla e con essa il proprietario tramite i pubblici registri., per cui la targa automobilistica può essere considera alla stregua di un dato personale.

È evidente che nella maggior parte dei casi l'indirizzo Ip non è in grado di consentire una immediata identificazione di una persona fisica (non è quindi un dato identificativo **forte**), anche in considerazione del fatto che generalmente gli Ip sono dinamici e quindi cambiano ad ogni connessione. Ma la norma ribadisce che è dato personale anche una informazione che consente di identificare una persona **indirettamente**, cioè incrociandola con altri dati, come, ad esempio l'orario di connessione, oppure l'accesso ad una postazione controllata (ad esempio in un internet point o in una biblioteca comunale o universitaria, ecc.). Tali dati, utilizzati insieme, consentono di identificare una persona fisica, grazie ai file di log del fornitore di connessione ad internet .

Pertanto come detto chiaramente da alcuni autori, l'indirizzo Ip non è sufficiente per condannare un soggetto per aver scaricato illecitamente un file, ma occorrono altri elementi "al fine di stabilire, eventualmente anche per presunzioni, che sia proprio quel soggetto e non altro, nell'ambito della ristretta

cerchia di coloro che hanno accesso a quella connessione internet, ad aver commesso quel reato. In assenza di prove non si può che giungere ad una sentenza di assoluzione, anche conoscendo l'Ip che identifica il computer dal quale è stato scaricato il file illecito".

Ergo: l'ip anche se considerato un dato personale --- > da solo potrebbe non essere in grado di identificare qualcuno.

Secondo il Parlamento Europeo, l'indirizzo IP è da classificarsi tra i dati personali e da trattarsi come tale, cioè in ossequio alle vigenti leggi sulla privacy.

In merito si è espresso anche l' articolo 29 (Data Protection Working Party che è un organo consultivo indipendente il quale riunisce le autorità per la protezione dei dati di tutta l'UE) che ha formulato un parere (documento 4 / 2007) sul Concetto di Dati Personali (WP 136).

Nel parere (**interamente riportato in Materiali di studio --- > vedere**) si analizzano i vari tipi di dati da considerarsi personali. Al punto 15 vengono considerati anche gli IP dinamici e si legge: "Esempio n. 15: Indirizzi IP dinamici - Il Gruppo considera gli indirizzi IP dati concernenti una persona identificabile. Al riguardo ha dichiarato che " *i fornitori di accesso Internet ei gestori delle reti LAN possono, utilizzando mezzi ragionevoli, identificare gli utenti Internet cui essi hanno attribuito indirizzi IP, poiché, normalmente, essi "registrano" in un apposito file la data, l'ora, la durata e l'indirizzo IP dinamico assegnato all'utente Internet. Lo stesso dicasi per i fornitori di servizi Internet, i quali detengono un registro sul server HTTP. In questi casi, non vi è dubbio sul fatto che si possa parlare di dati personali ai sensi dell'articolo 2 (a) della direttiva ...)"* .

Anche secondo il Garante l'indirizzo IP rientra tra i dati personali tant'è che nella propria "policy del sito" http://www.garanteprivacy.it/garante/doc.jsp?ID=36573) gli IP vengono inlcusi tra i dati personali dal Garante stesso.

La giurisprudenza: abbiamo visto che quella nazionale è piuttosto altalenante (vedi il caso Peppermint).

La giurisprudenza europea recentemente si è espressa a favore dell'IP come dato personale. Una sentenza emessa l'8 settembre 2010 dal Tribunale federale di Losanna (http://www.edoeb.admin.ch/aktuell/01688/index.html?lang=it) ha sancito che gli indirizzi IP devono essere considerati dati personali e pertanto devono sottostare alla legge sulla protezione dei dati. Il caso è simile al caso Peppermint per cui l'Alta Corte svizzera ha definito illecita la pratica di alcune imprese private che acquisiscono segretamente indirizzi IP al fine di verificare se utenti della rete commettono dei reati, nello specifico se scaricano file illeciti. "Secondo la Corte elvetica tale modo di agire non è giustificabile, per

cui ha vietato alla Logistep SA, appunto, di continuare la raccolta di dati personali degli utenti della rete.”

Secondo google, yahoo e altri motori di ricerca l’IP non puo’ essere considerato come dato personale. L'introduzione di una regola contraria creerebbe loro non pochi problemi. Infatti se l’IP venisse unanimemente e definitivamente considerato come dato personale sorgerebbero problemi per la sua archiviazione e per il suo trattamento da parte dei database dei motori di ricerca. Per questo motivo queste “aziende” sostengono che l'indirizzo IP non possa considerarsi come dato personale in quanto è un elemento estremamente labile, dato che può essere modificato, può essere "oscurato" tramite l'utilizzo di proxy, o può accadere che sia (apparentemente) impossibile associarlo ad un’unica identità, come nel caso di un internet point, laddove la macchina sia utilizzata da più utenti. A queste obiezioni si può rispondere facendo notare che anche una carta di identità può essere contraffatta ma ciò non toglie il suo valore giuridico identificativo verso il proprio titolare.

IN AMBITO DI BLOG

Per quanto riguarda l’anonimato nei blog si rinvia alla **lezione sui BLOG (vedere).**