SICUREZZA E PRIVACY
DAL PUNTO DI VISTA LEGALE

avv. Alessandro Nicotra – Firenze 30.11.2016

PREAMBOLO ED AVVERTENZE

- Questo “seminario” può causare fortissimi mal di testa …
- … il fatto che siate dirigenti, ricercatori, scienziati o che abbiate una doppia laurea in ingegneria aerospaziale ed in nanotecnologie potrebbe aiutare, ma…
- … nemmeno con l’ausilio di sostanze stupefacenti, infatti, potreste raggiungere gli inarrivabili livelli del moderno legislatore!
- Provocazioni e molta autoironia aiutano a districarsi meglio tra diritto, ricerca ed innovazione, così come un tipo di approccio non propriamente tradizionale...

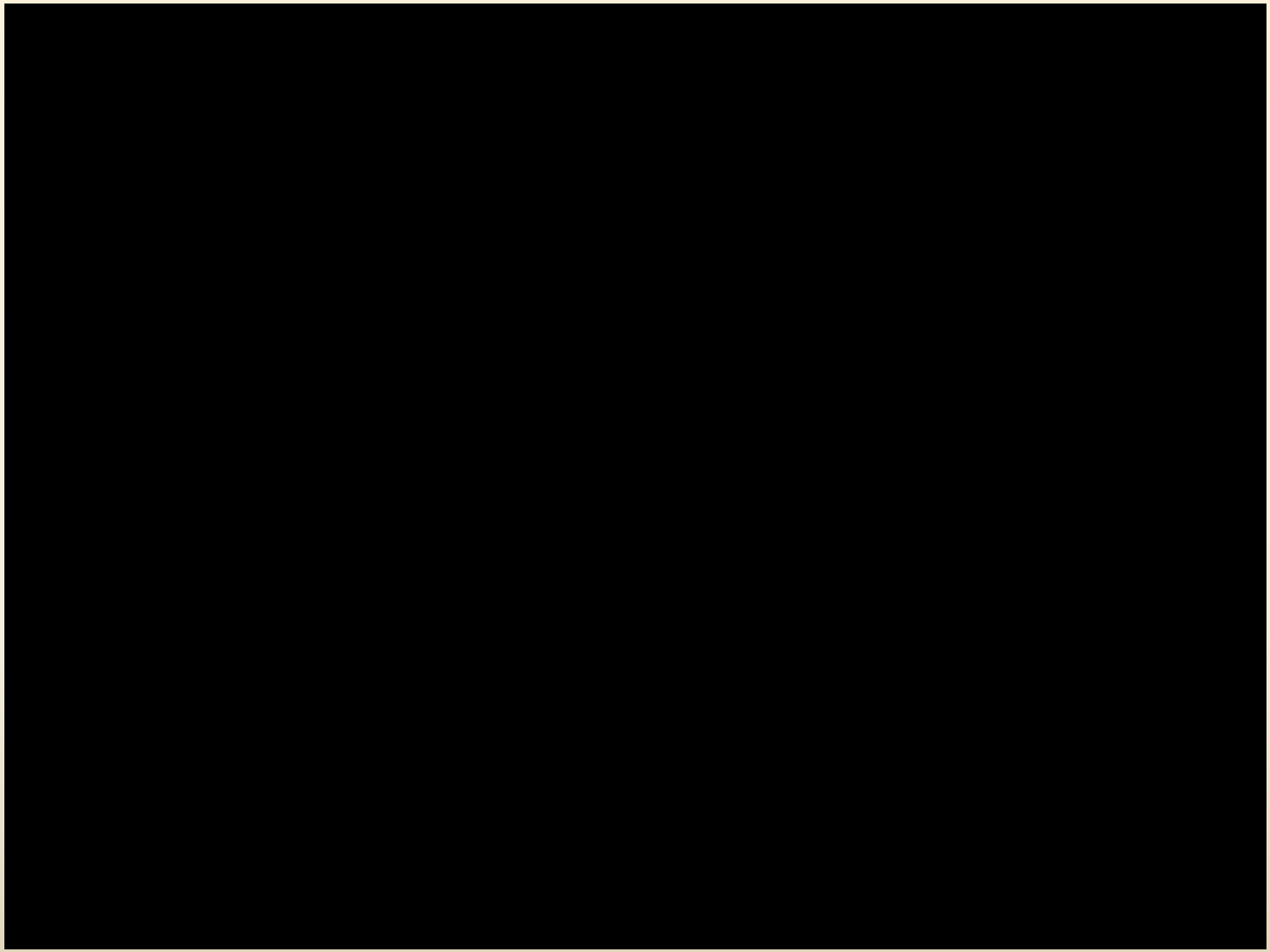
NON GUARDARMI: NON TI SENTO!

Tecnica e diritto sono su piani antitetici ed alieni?

Confrontiamo i “tempi” del diritto e dei suoi interpreti (siano essi legislatori, magistrati od avvocati) rispetto ai “tempi” dei transistori, fotografati dalla legge di Moore, che raddoppiano in velocità ed in capacità di elaborazione ogni 18 mesi.

Occorre comprendere e superare il disallineamento che si registra quando, da un lato si lavora su problematiche quali: identità digitale ed intelligenza artificiale… mentre dall’altro si fatica a distinguere la differenza tra PEC e firma digitale.

VELOCITÀ….



avv. Alessandro Nicotra – Firenze 30.11.2016

ANALFABETISMO FUNZIONALE?

Secondo l'Organizzazione per la Cooperazione e lo Sviluppo Economico (OCSE) il **47%** degli italiani non sarebbe capace di usare in modo efficace le proprie competenze di base ovvero lettura, scrittura e calcolo, risultando così "**analfabeta funzionale**"

SURFING vs. SNORKELING

Il mito dei cd. “nativi digitali” pare essere stato di recente sostituito dal più dispregiativo “millenials”…

…cyberbullismo, troyan, botnet, diffamazioni tramite social e, addirittura, le fake news che avrebbero determinato l’andamento delle presidenziali americane del 2016…

SURFING vs. SNORKELING

Ad una maggiore capacità di elaborazione delle informazioni (dati) da parte delle macchine non corrisponde un incremento della velocità di comprensione e ritenzione da parte umane, anzi…

Rem tene, verba sequentur?

SURFING vs. SNORKELING

Il problema, in prospettiva, non è legato solo ad una questione di "**memoria volatile**" ovvero all'atrofizzazione della capacità di memorizzare perché tanto ci pensa Siri, Cortana o Google…

Il problema è legato proprio a quelle capacità di comprensione che costituiscono il discrimine tra alfabetizzazione digitale ed analfabetismo funzionale.

Google Home Overview Features Services Learn | Google Wifi

Get to know Google Home.

Google Home is a voice-activated speaker powered by the Google Assistant. Ask it questions. Tell it to do things. It's your own Google, always ready to help. Just start with, "Ok Google".

WATCH VIDEO

SURFING vs. SNORKELING

Viviamo in una società iper connessa, ma proprio perché siamo tutti sempre più collegati ed “in Rete”, l’analfabetismo funzionale non deve essere considerato come un problema individuale, bensì come un’emergenza sociale.

Basti pensare alla sicurezza informatica.

PERCEZIONE

L’intelligenza umana si nutre di conoscenza, la conoscenza di esperienza (diretta od indiretta), l’esperienza passa attraverso la percezione: l’uomo conosce attraverso i propri sensi, ma anche attraverso i propri stati d’animo.

Dematerializzata o digitalizzata l’informazione una piccola provocazione:

può essere de materializzata la… percezione?

PERCEZIONE

Questioni distopiche e domande filosofiche?

Si pensi a quale sia la **percezione** più diffusa in relazione a quello che si fa con lo smartphone o con Internet (per esempio dallo scaricare al caricare materiale audio-video)…

o la percezione tra identità e firma digitale rispetto alle potenziali conseguenze…

… e perché il diritto si è dovuto spingere ad elaborare il concetto di diritto all'oblio.

PERCEZIONE

La stessa fisica quantistica discute di oggetto osservato influenzato dall'osservatore.

Si pensi al "**gatto di Schroedinger**" (il celebre esempio in cui un gatto è contemporaneamente vivo e morto finché non lo si osserva) e si pensi a come viene inteso dai più il cd. "mondo virtuale"

PERCEZIONE

Quello che per uno scienziato od un tecnologo è un problema di prospettiva, di calcolo, di tele-medicina, di ingegneria molecolare, di fisica meccanica o quantistica …

… per il giurista diventa una questione speculativa, sociale e di convivenza da dover in qualche modo regolamentare (o nelle sue **cause** o nei suoi **effetti**).


© Facebook

WYSIWYG

*Zuckerberg ha annunciato la sua sfida: rendere il suo **Gear VR un oggetto sociale**, che permetta ad "amici che vivono in differenti parti del mondo, di trascorrere del tempo assieme, come se fossero davvero vicini". Zuckerberg ha finalmente spiegato cosa lo ha spinto a comprare Oculus due anni fa per due miliardi di dollari. Non certo per continuare a sviluppare giochi per nerd. Ma per avvicinare sempre più Oculus al concetto principe di Facebook: **far connettere le persone**.* (tratto da *http://www.wired.it/gadget/accessori/2016/02/22/zuckerberg-foto*/)

WYSIWYG

“connettere le persone” ?

WYSIWYG

Ok, forse Zuckerberg non ha in mente il film di fantascienza “the Matrix” (1999) quando parla di **connettere le persone**…, ma resta la domanda: **perché?**

L’idea è davvero quella di poter condividere, interagire e “*trascorrere del tempo assieme*” azzerando le distanze, come se si fosse vicini?


STRONGER TOGETHER
STRONGER TOGETHER
STRONGER TOGETHER
STRONGER TOGETHER

ibis redibis non morieris in bello

Quando l'**attenzione** a dove mettere la virgola (e magari la testa) ti può salvare la vita:

informazione -> velocità -> percezione -> comprensione -> valutazione -> azione/reazione

Il legislatore dovrebbe essere "quello che mette le virgole" ma… (o che qualcuno bara o che lui non capisce) …sembra sempre un passo indietro

velocità…

CAUSE - EFFETTI

Stiamo assistendo ad un progresso tecnologico così veloce da stravolgere qualsiasi legge, persino quelle della fisica.

Solo per fare qualche esempio concreto a riguardo: giurisdizione, tributi, identificazione…

…e mentre stiamo ancora ragionando su quelli, già si affacciano le questioni relative a IoT, AI, VR

CAUSE - EFFETTI

Per discutere di sicurezza e riservatezza oggi, bisognerebbe prima partire da quello che scriveva Dante nel canto V del Paradiso:

"***non fa scienza, sanza lo ritenere, avere inteso***"

Il diritto, in realtà, oggi "insegue". Non solo: accade a volte che venga interpretato "*sanza lo ritenere, avere inteso*" e soprattutto senza "scienza" ovvero senza le cognizioni tecniche.

CAUSE - EFFETTI

L'overload di dati ed informazioni manda in tilt sia cervelli umani che elettronici: con il **sovraccarico cognitivo** e con il **denial of service.**

IL CONTROLLO

Se da un lato sembra essere il legislatore od il giurista ad arrancare nel tentativo di regolamentare ed interpretare le innovazioni…

…dall'altro il problema del controllo attanaglia anche tecnici e scienziati, sia sotto il profilo della sicurezza che sotto quello della responsabilità.

IL CONTROLLO

ovvero l'incubo del

… "non potevi non sapere" …

… amianto, terremoti, sicurezza,

infrastrutture critiche, perdita di dati …

-> **prudenza** <- e -> **responsabilità** <-

avv. Alessandro Nicotra – Firenze 30.11.2016

IL CONTROLLO

… e quando hai fatto tutto,

ma proprio tutto,

come si deve…

…casca un albero sulla rete elettrica tra Italia e Svizzera come nel Black-out del sistema elettrico italiano del 28 settembre 2003!

CASO FORTUITO e FORZA MAGGIORE

Art. 2043 c.c.

"Qualunque fatto doloso o colposo, che cagiona ad altri un danno ingiusto, obbliga colui che ha commesso il fatto a risarcire il danno"

Il **caso fortuito** indica un evento assolutamente imprevedibile. La **forza maggiore** indica un evento di una forza tale alla quale non è oggettivamente possibile resistere

CASO FORTUITO e FORZA MAGGIORE

entrambi hanno come effetto l'esclusione della responsabilità del soggetto agente

…ed incidentalmente, anche nel diritto penale…

…vi è l'articolo 45 c.p. che attesta come non punibile penalmente chi ha commesso il fatto illecito per caso fortuito o per forza maggiore.

RESPONSABILITÀ

Se prescindiamo da qualsivoglia considerazione etico-religiosa, limitandoci a rimanere nei confini del cosiddetto diritto positivo e dell'umanamente prevedibile, le responsabilità cui è possibile andare incontro sono di tipo:

civile, penale od amministrativo.

RESPONSABILITÀ

Il concetto di responsabilità si può considerare trasversale al mondo del diritto anglosassone rispetto ai sistemi di civil law come il nostro.

Al contrario concetti come “riservatezza” o “privacy” possono assumere significati e rilevanza completamente diversi (indisponibilità vs. valorizzazione meramente economica).

DATA PROTECTION

Se accettiamo il presupposto comune legato al concetto di “responsabilità”…

Ecco l’undicesimo comandamento:

“Proteggere i dati!!!”

l’origine, il trattamento, la conservazione

(perché noi… non possiamo non sapere)

DATA PROTECTION

Dal punto di vista giuridico, sintetizzando estremamente, si può affermare che rilevano, soprattutto sotto il profilo della responsabilità:

-le cause (perché raccolgo, tratto, uso i dati, etc.)

- gli effetti (come li tratto e li conservo, misure di sicurezza, prevenzione, etc.)

ALCUNI RIFERIMENTI LEGISLATIVI

L. 23 dicembre 1993 n. 547 “Modificazioni ed integrazioni alle norme del codice penale e del codice di procedura penale in tema di criminalità informatica”;

- D.Lgs. 8 giugno 2001, n. 231 “Disciplina della responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica”;
- D.Lgs.30 giugno 2003, n. 196 “Codice in materia di protezione dei dati personali”;
- D.Lgs. 7 marzo 2005, n. 82 “Codice dell’amministrazione digitale” e successive modifiche sino al D.Lgs.179/2016);
- il FOIA (freedom od information act)…….

ALCUNI RIFERIMENTI LEGISLATIVI

FOIA ovvero Decreto Legislativo del 17 maggio 2016 recante la

REVISIONE E SEMPLIFICAZIONE DELLE DISPOSIZIONI IN MATERIA DI PREVENZIONE DELLA CORRUZIONE PUBBLICITA' E TRASPARENZA **CORRETTIVO DELLA LEGGE 6 NOVEMBRE 2012, N. 190 E DEL DECRETO LEGISLATIVO 14 MARZO 2013, N. 33**, AI SENSI DELL'ARTICOLO 7 DELLA LEGGE 7 AGOSTO 2015, N. 124, IN MATERIA DI RIORGANIZZAZIONE DELLE AMMINISTRAZIONI PUBBLICHE

IL CODICE DELL'AMMINISTRAZIONE DIGITALE

Il CAD traccia il quadro legislativo entro cui deve attuarsi la digitalizzazione dell'azione amministrativa e sancisce veri e propri diritti dei cittadini e delle imprese in materia di uso delle tecnologie nei rapporti con le Amministrazioni

Il CAD contiene anche l'obbligo per l'Amministrazione di snellire le procedure e di rendere tutti i servizi e le comunicazioni interne ed esterne per via telematica

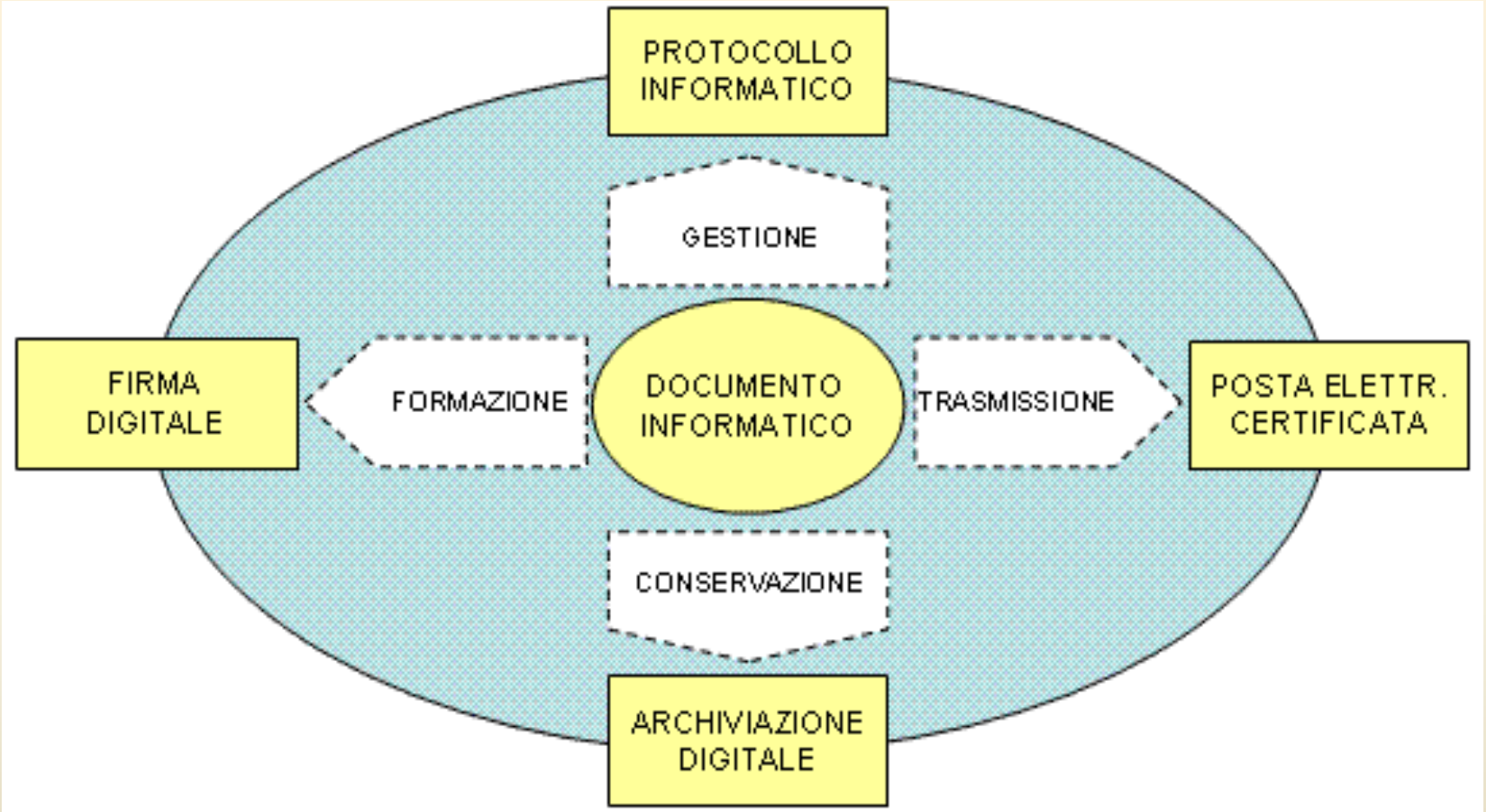
IL CODICE DELL'AMMINISTRAZIONE DIGITALE

Il testo del Codice dell'Amministrazione Digitale è stato oggetto di numerosi interventi di modifica ed aggiornamento da parte del legislatore: si segnalano, in particolare, le novelle rappresentate dal D. Lgs. n. 235/2010 (c.d. "nuovo CAD", dal D.L. n. 179/2012 (c.d. "Agenda Digitale Italiana") che hanno reso ancor più stringenti gli obblighi per le Amministrazioni ed infine dal **D.Lgs.179/2016** che ha però creato anche alcune perplessità agli interpreti.

IL CODICE DELL'AMMINISTRAZIONE DIGITALE

- Digitalizzazione dell'attività amministrativa
- Rapporti tra pubbliche amministrazioni e imprese
- Trasparenza
- Pagamenti informatici
- Firme digitali
- Customer satisfaction
- Utilizzo della posta elettronica certificata
- Dematerializzazione dei documenti
- Protocollo informatico e fascicolo elettronico
- Conservazione dei documenti
- Accesso ai servizi in rete
- Istanze alle pubbliche amministrazioni
- Continuità operativa e disaster recovery
- Scambi di dati
- Dati pubblici

IL CODICE DELL'AMMINISTRAZIONE DIGITALE



IL CODICE DELLA PRIVACY

Il Codice in materia di protezione dei dati personali (artt. da 33 a 36 del Codice) con il famigerato **allegato B** detta il "**Disciplinare tecnico in materia di misure minime di sicurezza**" ovvero le modalità tecniche da adottare a cura del titolare, del responsabile ove designato e dell'incaricato, in caso di trattamento con strumenti elettronici.

IL CODICE DELLA PRIVACY

In caso di trattamento di dati sensibili o giudiziari:

20**. I dati sensibili o giudiziari sono protetti contro l'accesso abusivo, di cui all'art. 615-ter del codice penale, mediante l'utilizzo di idonei strumenti elettronici.**
21. Sono impartite istruzioni organizzative e tecniche per la custodia e l'uso dei supporti rimovibili su cui sono memorizzati i dati al fine di evitare accessi non autorizzati e trattamenti non consentiti.
22. I supporti rimovibili contenenti dati sensibili o giudiziari se non utilizzati sono distrutti o resi inutilizzabili, ovvero possono essere riutilizzati da altri incaricati, non autorizzati al trattamento degli stessi dati, se le informazioni precedentemente in essi contenute non sono intelligibili e tecnicamente in alcun modo ricostruibili.
23**. Sono adottate idonee misure per garantire il ripristino dell'accesso ai dati in caso di danneggiamento degli stessi o degli strumenti elettronici, in tempi certi compatibili con i diritti degli interessati e non superiori a sette giorni**.
24. Gli organismi sanitari e gli esercenti le professioni sanitarie effettuano il trattamento dei dati idonei a rivelare lo stato di salute e la vita sessuale contenuti in elenchi, registri o banche di dati con le modalità di cui all'articolo 22, comma 6, del codice, anche al fine di consentire il trattamento disgiunto dei medesimi dati dagli altri dati personali che permettono di identificare direttamente gli interessati.
I dati relativi all'identità genetica sono trattati esclusivamente all'interno di locali protetti accessibili ai soli incaricati dei trattamenti ed ai soggetti specificatamente autorizzati ad accedervi; il trasporto dei dati all'esterno dei locali riservati al loro trattamento deve avvenire in contenitori muniti di serratura o dispositivi equipollenti; il trasferimento dei dati in formato elettronico è cifrato.

IL CODICE DELLA PRIVACY

Art. 33. Misure minime

1. Nel quadro dei più generali obblighi di sicurezza di cui all'articolo 31, o previsti da speciali disposizioni, i titolari del trattamento sono comunque tenuti ad adottare le misure minime individuate nel presente capo o ai sensi dell'articolo 58, comma 3, volte ad assicurare un livello minimo di protezione dei dati personali.

Art. 34. Trattamenti con strumenti elettronici

1. Il trattamento di dati personali effettuato con strumenti elettronici è consentito solo se sono adottate, nei modi previsti dal disciplinare tecnico contenuto nell'allegato B), le seguenti misure minime:

a) autenticazione informatica;

b) adozione di procedure di gestione delle credenziali di autenticazione;

c) utilizzazione di un sistema di autorizzazione;

d) aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici;

e) protezione degli strumenti elettronici e dei dati rispetto a trattamenti illeciti di dati, ad accessi non consentiti e a determinati programmi informatici;

f) adozione di procedure per la custodia di copie di sicurezza, il ripristino della disponibilità dei dati e dei sistemi;

g) [soppressa];

h) adozione di tecniche di cifratura o di codici identificativi per determinati trattamenti di dati idonei a rivelare lo stato di salute o la vita sessuale effettuati da organismi sanitari.

1-bis. [abrogato]

1-ter. Ai fini dell'applicazione delle disposizioni in materia di protezione dei dati personali, i trattamenti effettuati per finalità amministrativo-contabili sono quelli connessi allo svolgimento delle attività di natura organizzativa, amministrativa, finanziaria e contabile, a prescindere dalla natura dei dati trattati. In particolare, perseguono tali finalità le attività organizzative interne, quelle funzionali all'adempimento di obblighi contrattuali e precontrattuali, alla gestione del rapporto di lavoro in tutte le sue fasi, alla tenuta della contabilità e all'applicazione delle norme in materia fiscale, sindacale, previdenziale-assistenziale, di salute, igiene e sicurezza sul lavoro.

Art. 35. Trattamenti senza l'ausilio di strumenti elettronici

1. Il trattamento di dati personali effettuato senza l'ausilio di strumenti elettronici è consentito solo se sono adottate, nei modi previsti dal disciplinare tecnico contenuto nell'allegato B), le seguenti misure minime:

a) aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unità organizzative;

b) previsione di procedure per un'idonea custodia di atti e documenti affidati agli incaricati per lo svolgimento dei relativi compiti;

c) previsione di procedure per la conservazione di determinati atti in archivi ad accesso selezionato e disciplina delle modalità di accesso finalizzata all'identificazione degli incaricati.

Art. 36. Adeguamento

1. Il disciplinare tecnico di cui all'allegato B), relativo alle misure minime di cui al presente capo, è aggiornato periodicamente con decreto del Ministro della giustizia di concerto con il Ministro per le innovazioni e le tecnologie e il Ministro per la semplificazione normativa, in relazione all'evoluzione tecnica e all'esperienza maturata nel settore.

U.E.

Dal titolo si potrebbe pensare ad un inizio di pianto, ma no…

… in questa presentazione ci riferiamo alla cara vecchia Unione Europea che ci ha regalato di recente direttive come eIDAS ed il Regolamento Europeo sulla privacy.

Il Regolamento UE n° 910/2014 - eIDAS

Il Regolamento eIDAS (electronic IDentification Authentication and Signature) - **Regolamento UE n° 910/2014 sull'identità digitale** - ha l'obiettivo di fornire una base normativa a livello comunitario per i servizi fiduciari e i mezzi di identificazione elettronica degli stati membri.

Il regolamento eIDAS ha l'obiettivo di rafforzare la fiducia nelle transazioni nell'Unione Europea, fornendo una base normativa comune per interazioni elettroniche sicure fra cittadini, imprese e pubbliche amministrazioni.

Ha inoltre lo scopo di aumentare la sicurezza e l'efficacia dei servizi elettronici, nonché delle transazioni di e-business e commercio elettronico nell'Unione Europea.

Il Regolamento UE n° 910/2014 - eIDAS

Il regolamento, “allo scopo di garantire il buon funzionamento del mercato interno perseguendo al contempo un adeguato livello di sicurezza dei mezzi di identificazione elettronica e dei servizi fiduciari:

- fissa le condizioni a cui gli Stati membri riconoscono i mezzi di identificazione elettronica delle persone fisiche e giuridiche che rientrano in un regime notificato di identificazione elettronica di un altro Stato membro,
- stabilisce le norme relative ai servizi fiduciari, in particolare per le transazioni elettroniche;
- istituisce un quadro giuridico per le firme elettroniche, i sigilli elettronici, le validazioni temporali elettroniche, i documenti elettronici, i servizi elettronici di recapito certificato e i servizi relativi ai certificati di autenticazione di siti web.”

Il Regolamento UE n° 910/2014 - eIDAS

Rispetto ai sistemi di identificazione elettronica, infatti, il regolamento prevede che ciascuno Stato membro possa notificare i sistemi di identificazione elettronica forniti ai cittadini e alle aziende ai fini del mutuo riconoscimento.

In quest'ottica, particolare rilevanza assume anche la piena interoperabilità a livello comunitario di particolari tipologie di firme elettroniche e dei sistemi di validazione temporale note in Italia rispettivamente come firma digitale e marca temporale.

Il Regolamento UE 2016/679 (data protection o privacy)

Il titolo esatto è : ” Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, **relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati** e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati) ”

Vi è poi la **Direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio, del 27 aprile 2016**, relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio

Il Regolamento UE 2016/679 (data protection o privacy)

Il **5 maggio 2016** è entrata ufficialmente in vigore la Direttiva, che dovrà essere recepita dagli Stati membri entro 2 anni.

Il **24 maggio 2016** è entrato ufficialmente in vigore il Regolamento, che diventerà definitivamente applicabile in via diretta in tutti i Paesi UE a partire dal **25 maggio 2018**.

Il Regolamento UE 2016/679

Il Regolamento introduce regole più chiare in materia di informativa e consenso, definisce i limiti al trattamento automatizzato dei dati personali, pone le basi per l'esercizio di nuovi diritti, stabilisce criteri rigorosi per il trasferimento dei dati al di fuori dell'Ue e per i casi di violazione dei dati personali (data breach).

Il titolare del trattamento dovrà comunicare eventuali violazioni dei dati personali (data breach) all'Autorità nazionale di protezione dei dati. Se la violazione dei dati rappresenta una minaccia per i diritti e le libertà delle persone, il titolare dovrà informare in modo chiaro, semplice e immediato anche tutti gli interessati e offrire indicazioni su come intende limitare le possibili conseguenze negative.

Il Regolamento UE 2016/679

Il Regolamento promuove la responsabilizzazione (*accountability*) dei titolari del trattamento e l'adozione di approcci e politiche che tengano conto costantemente del rischio che un determinato trattamento di dati personali può comportare per i diritti e le libertà degli interessati. Il principio-chiave è «**privacy by design**», ossia garantire la protezione dei dati fin dalla fase di ideazione e progettazione di un trattamento o di un sistema, e adottare comportamenti che consentano di prevenire possibili problematiche.

Il Regolamento UE 2016/679

Ad esempio, è previsto l'obbligo di effettuare valutazioni di impatto prima di procedere ad un trattamento di dati che presenti rischi elevati per i diritti delle persone, consultando l'Autorità di protezione dei dati in caso di dubbi. Viene inoltre introdotta la figura del «Responsabile della protezione dei dati» (Data Protection Officer o DPO), incaricato di assicurare una gestione corretta dei dati personali nelle imprese e negli enti. In compenso, scompaiono alcuni oneri amministrativi come l'obbligo di notificare particolari trattamenti, oppure di sottoporre a verifica preliminare dell'Autorità i trattamenti considerati «a rischio».

il CERT nazionale Italia

Per garantire capacità di prevenzione e reazione ad eventi cibernetici si è ritenuto necessario promuovere lo sviluppo di CERT (Computer Emergency Response Team) quali soggetti erogatori di servizi di supporto, formazione, informazione, ricerca e sviluppo per i rispettivi utenti, pubblici o privati.

Il CERT Nazionale (https://www.certnazionale.it/) supporta la costituzione di una community per la sicurezza nazionale.

RFC2350 fornisce il profilo del Cert nazionale Italia e di come possa essere contattato.

il CERT nazionale

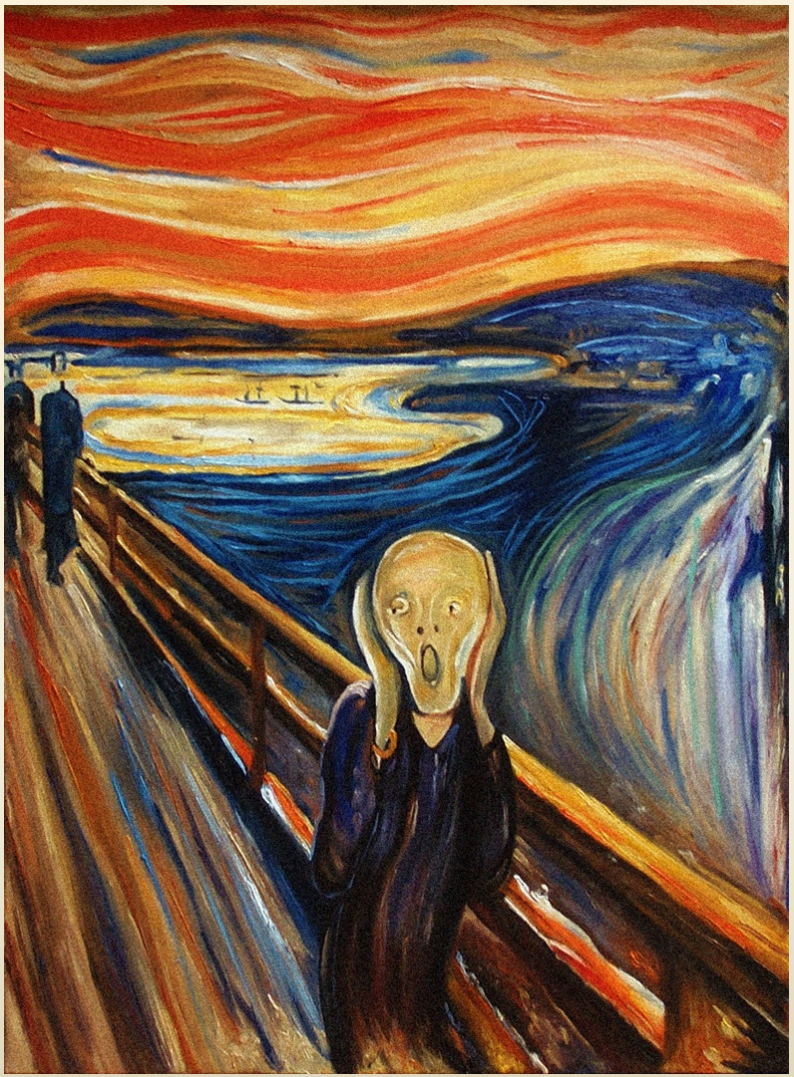
I riferimenti normativi del CERT nazionale italiano sono:

- il **Decreto Legislativo 1 agosto 2003 n. 259** recante il Codice delle comunicazioni elettroniche, modificato dal **Decreto Legislativo 28 maggio 2012 n. 70** (attuazione delle direttive **2009/140/CE**) all'art. 16bis comma 4 prevede l'individuazione del CERT Nazionale presso il **Ministero dello Sviluppo Economico**, con compiti di prevenzione e di supporto a cittadini ed imprese nel fronteggiare incidenti informatici;

- il **DPCM 24 gennaio 2013**, che ha delineato l'architettura istituzionale per la protezione cibernetica e la sicurezza informatica nazionale, ha affidato al CERT Nazionale la funzione di supporto al Tavolo NISP – Nucleo Interministeriale Situazione e Pianificazione, che agisce come "Tavolo interministeriale di Crisi Cibernetica";

- il **DPCM 158 del 2013**, che affida all'Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione le attività di pertinenza del CERT Nazionale (art. 14).

CONCLUSIONI…



CONCLUSIONI…

Ricapitolando:

l'informazione si de materializza in bit che viaggiano a velocità spesso superiori alle capacità di ritenzione e comprensione dei singoli. Il diritto, chiamato a regolamentare e tutelare, prova a fissare dei paletti, ma gli stessi interpreti del diritto mostrano di aver bisogno di maggiore formazione o supporto tecnico. Il concetto di sicurezza, spesso collegato ad una mera percezione e basato sulla fiducia, diventa sempre più ricollegato al concetto di Sicurezza informatica e all'utilità personale…

CONCLUSIONI…

E la sicurezza informatica non riguarda solo la raccolta ed il trattamento dei dati (privacy), ma anche i mezzi di trasmissione e di pagamento, l'affidabilità e la regolamentazione dei sistemi automatizzati (AI, robot, veicoli a movimentazione autonoma, etc.)

Una sfida che non è più soltanto tecnologica ma che deve coinvolgere sin da subito anche formatori e giuristi al fine di progettare ed individuare (by design) soluzioni e modalità più sicure con un occhio alla salvaguardia della dignità umana (riservatezza e diritto all'oblio) e l'altro al progresso.

Grazie…

…per l’attenzione e la pazienza

avv. Alessandro Nicotra

alenico@gmail.com