Normativa applicabile all'IT

Cesare Gallotti

2021-01-09

Cesare Gallotti

Agenda

- Computer Crime
- Diritto d'autore
- Dlgs 231
- Accessibilità
- E-Commerce
- Amministrazione digitale
- Infrastrutture critiche e segreto di stato
- Operatori di TLC e ISP
- Finance
- Privacy
- Sicurezza fisica
- Varie normative
- Per aggiornarsi

- Le novità dal gennaio 2018 sono evidenziate da un bollino: 

Computer Crime

Riferimenti normativi

- Riferimenti:
  - Legge 547 del 1993;
  - Dlgs 373 del 2000;
  - Legge 48 del 2008;
  - Legge 71 del 2017 (Legge sul cyberbullismo).
- Questa normativa riguarda reati specifici quali l'accesso abusivo ai sistemi IT, la diffusione di virus, il danneggiamento di sistemi IT, eccetera.
- Nessuna azienda ha il dovere di fare alcunché, se non sensibilizzare il proprio personale in merito affinché non commetta questi reati, per cui anche l'organizzazione potrebbe essere ritenuta responsabile (vedere discussione su Dlgs 231).
- La Legge 48 regolamenta parzialmente la Computer Forensics.

Computer forensics

- La Legge 48 regolamenta questo settore da un punto di vista penale.
- Le tecniche di Computer Forensics sono diverse e variegate, anche in funzione dei sistemi oggetto di analisi (pc accesi o spenti, cellulari, server attivi e server che non possono essere disattivati).
- L'informatico da solo non ha gli strumenti (competenze) per occuparsi autonomamente della raccolta e analisi delle prove. Questo perché le sue risultanze dovranno poi essere utilizzate da avvocati o dalle Forze dell'Ordine, ognuno con le proprie specificità.
- Per le organizzazioni, si può suggerire di redigere delle linee guida, in collaborazione con l'Ufficio Legale, per il trattamento dei casi di "computer forensics": la prima mossa è comunque la disconnessione del pc o del server dalla rete (se necessario per bloccare delle azioni) e l'impedimento di qualsiasi suo utilizzo.

Statuto dei Lavoratori

- L’articolo 4 della Legge 300 del 1970 è stato modificato a settembre 2015
  - Il comma 1 dice che è possibile utilizzare strumenti di controllo purché con le opportune autorizzazioni (RSU, rappresentanze sindacali, Direzione territoriale del lavoro). Gli strumenti di controllo "possono essere installati solo per esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio aziendale". Si suppone che le "esigenze produttive" non includano il controllo delle prestazioni del singolo lavoratore, ma solo quelle "generali".
  - Il comma 2 dice che il comma 1 non si applica "agli strumenti utilizzati dal lavoratore per rendere la prestazione lavorativa e agli strumenti di registrazione degli accessi e delle presenze" e quindi non sono necessarie specifiche autorizzazioni (da usare solo le funzionalità di «base».
  - Il comma 3 richiede che il datore di lavoro, in tutti i casi, informi i lavoratori delle modalità di controllo.
  - Nota: la giurisprudenza ha normalmente approvato i controlli "reattivi", ossia avviati dopo che sono stati segnalati potenziali illeciti da parte di singole persone.
  - Nota. Il Consiglio d'Europa, in data 1° aprile 2015, ha adottato la Raccomandazione CM/Rec(2015)5 sul trattamento dei dati personali nel contesto dell'occupazione. Ancora da capire come integrare queste disposizioni con quelle già in essere in Italia.

Diritto d’autore

Riferimenti normativi

- La normativa in vigore in materia di Diritto d'Autore è la Legge 633 del 1941 (promulgata dal Re d'Italia e di Albania e Imperatore d'Etiopia!).
- Questa Legge è stata oggetto di moltissimi cambiamenti, spesso difficili da consolidare.
- È di interesse anche il Codice di Proprietà Industriale (Dlgs 30 del 2005) e il suo regolamento di attuazione (Decreto Ministero Sviluppo Economico n. 33 del 2010).
- NUOVO Le aziende dovrebbero stabilire chiaramente quali informazioni sono proprietarie ("segreti commerciali") – da DL 63 del 2018.
- Anche i software e le banche dati sono coperte dal Diritto d'Autore.
- Standard parzialmente dedicato alla gestione delle licenze software è oggetto dello standard ISO/IEC 19770 (ma anche altri standard lo trattano).
- Nessuna azienda deve "mettere in atto" azioni per rispettare il Diritto d'Autore, deve però evitare comportamenti illeciti.

Punti chiave

- E’ possibile verificare se:
  - è realizzato un sistema di censimento delle licenze;
  - è attivo un sistema di discovery dei software installati;
  - sono attivati allarmi nel caso in cui sia individuato software installato non previsto;
  - siano impostati controlli tra software installato e licenze acquisite;
  - sono gestite le “prove di licenza” (ossia dei documenti che attestano le licenze attive).
- L’ultimo punto è relativamente semplice da affrontare, gli altri sono complessi perché sono presenti tanti tipi di software e tanti tipi di licenze anche per uno stesso software.
- Verificare la presenza del bollino SIAE sui CD o DVD venduti (DPCM 31 del 2009).
- NUOVO Se sono chieste agevolazioni fiscali, l’elenco degli asset dichiarati all’Agenzia delle entrate, se in ambito, deve essere allineato a quello usato per la valutazione del rischio e all’inventario degli asset (“Patent Box”, L. 190/2014).

Dlgs 231

Responsabilità Amministrativa delle Imprese

Riferimenti Normativi

- Riferimento: Dlgs 231 del 2001
  - Altri riferimenti:
    - Linee Guida di Confindustria del 2014 (aggiornano quelle del 2008).
- Il principio è il seguente:
  - L'ente (ossia l'organizzazione) è responsabile per i reati commessi nel suo interesse o a suo vantaggio.
- Nessun ente è obbligato a realizzare misure di conformità alla 231. E' facoltativo e di garanzia per i "soggetti in posizione apicale".
- Alcuni la definiscono "la SOX (Sarbanes – Oxley) italiana", per la quale valgono principi simili, ma molto legati alla sicurezza sistemi organizzativi e informatici di contabilità (ambito tradizionalmente poco trattato dai sistemi di gestione ISO).

Reati da 231

- Alcuni reati trattati dalla 231 e collegati all'informatica:
  - Art. 24. Indebita percezione di erogazioni, truffa in danno dello Stato o di un ente pubblico o per il conseguimento di erogazioni pubbliche e frode informatica in danno dello Stato o di un ente pubblico;
  - Art. 24-bis - Delitti informatici e trattamento illecito di dati (introdotto dalla 48/2008);
  - Art. 25 - Concussione e corruzione;
  - Art. 25-bis - Falsità in monete, in carte di pubblico credito e in valori di bollo (Aggiunto dal DL 350 del 2001);
  - Art. 25-bis - Falsità in [...]strumenti o segni di riconoscimento (Aggiunto dalla Legge 99 del 2009);
  - Art. 25-bis.1. - Delitti contro l'industria e il commercio (Aggiunto dalla Legge 99 del 2009);
  - Articolo 25-ter - Reati societari (Aggiunto dal Decreto Legislativo 61 del 2002);
  - Articolo 25-quater - Delitti con finalità di terrorismo o di eversione dell'ordine democratico (Aggiunto dalla Legge 7 del 2003);
  - Articolo 25-quinques - Delitti contro la personalità individuale (Aggiunto dalla Legge 228 del 2003 e modificato dalla Legge 38 del 2006);
  - Articolo 25-sexies - Abusi di mercato (Aggiunto dalla Legge 62 del 2005);
  - Articolo 25-septies. - Omicidio colposo e lesioni colpose gravi o gravissime, commessi con violazione delle norme antinfortunistiche e sulla tutela dell'igiene e della salute sul lavoro (Aggiunto dalla Legge 123 del 2007);
  - Art. 25- novies - Delitti in materia di violazione del diritto d'autore.

Punti di attenzione

- Se l'impresa ha attivato un "sistema 231", verificare quanto segue:
  - se è stato considerato anche dal SGQ-SGSI-ITSMS;
  - se i rapporti dell'Organismo di Vigilanza hanno avuto impatti sul SGQ-SGSI-ITSMS;
  - se la Politica del SGQ-SGSI-ITSMS è in linea con il Disciplinare utenti.

Accessibilità

Legge Stanca

- Riferimenti:
  - Legge 9 gennaio 2004, n.4 “Disposizioni per favorire l’accesso dei soggetti disabili agli strumenti informatici”;
  - DPR 75 del 2005 Regolamento di attuazione della legge Stanca;
  - Decreto del Ministro per l’Innovazione e le Tecnologie dell’8 luglio 2005 “Requisiti tecnici e i diversi livelli per l'accessibilità agli strumenti informatici”.
- Altri riferimenti:
  - http://www.agid.gov.it (dal 2012 ha incorporato DigitPA, già CNIPA);
  - Quaderno 4 del 2005 del CNIPA “La Legge Stanca: i riferimenti tecnici”;
  - http://www.w3.org/WAI/.
- La Legge Stanca si applica alle pubbliche amministrazioni, agli enti pubblici economici, alle aziende private concessionarie di servizi pubblici, alle aziende municipalizzate regionali, agli enti di assistenza e di riabilitazione pubblici, alle aziende di trasporto e di telecomunicazione a prevalente partecipazione di capitale pubblico e alle aziende appaltatrici di servizi informatici.

Punti chiave

- Questo riferimento riguarda la qualità.
- Nei requisiti di ingresso alla progettazione, dove applicabile, devono essere presi in carico i requisiti di accessibilità per i disabili.
- Anche alcune aziende private si sono prese in carico i requisiti di accesso per i disabili. È possibile richiedere una “certificazione” dell’accessibilità del proprio sito.
- I requisiti riguardano:
  - applicazioni basate su tecnologie internet (requisiti ISO, W3C o altro);
  - personal computer;
  - ambiente operativo, le applicazioni e i prodotti a scaffale.

E-Commerce

Riferimenti normativi

- Riferimenti normativi:
  - Dlgs 70 del 2003;
  - Dlgs 206 del 2005: “Codice del consumo” (aggiornato con D.lgs. 21 del 2014 e altri);
  - Dlgs 69/2012 (riferimenti pubblicitari o meno a siti web devono essere a siti conformi alle prescrizioni del Dlgs 70 del 2003);
  - NUOVO EU Digital content directive (770 e 771 del 2019), da recepire entro giugno 2021, sul commercio elettronico di beni digitali.
- Altri riferimenti più specifici riguardano:
  - la commercializzazione di servizi finanziari (Dlgs 190 del 2005);
  - i regolamenti sui giochi on-line (decreti dell’AAMS, www.aams.gov.it).
- Attenzione che i siti web sono soggetti alla normativa sull’editoria;
  - il gestore di sito web è responsabile anche per i commenti.

Punti chiave

- Per quanto riguarda la qualità, verificare che:
  - siano fornite in modo semplice e chiaro i dati sul prestatore (Art. 7 del Dlgs 70), incluse le modalità di contatto;
  - le condizioni contrattuali siano facilmente reperibili;
  - le comunicazioni commerciali via e-mail includano la clausola di “rescissione”;
  - è pubblicato un codice di condotta;
  - il cliente può recidere il contratto (normalmente entro 2 giorni, per il Codice del Consumo).
- Per la sicurezza:
  - verificare che siano stati considerate le “normali” misure di sicurezza per un sito di e-commerce.
- Per la qualità e la sicurezza:
  - l’operatore di hosting deve essere reperibile per ricevere comunicazioni di attività illegali (es. diritto d’autore) e cancellare quanto necessario.

Codice del consumo

- Dal 2014 sono state introdotte novità al Codice del Consumo per i contratti a distanza.
- In sintesi:
  - obbligo di informativa precontrattuale più gravoso rispetto al precedente e di forma scritta;
  - diritto di ripensamento: il consumatore può recedere dall'acquisto entro 14 giorni ma se l'informativa è incompleta ha 12 mesi;
  - restituzione del prodotto: il consumatore ha la possibilità di restituire il prodotto, anche se deteriorato.
- Articolo di Filodiritto: http://www.filodiritto.com/contratti-tra-consumatori-e-professionisti-litalia-recepisce-la-direttiva-europea-e-modifica-il-codice-del-consumo

Firma contratti

- «Tribunale di Catanzaro - Sezione Prima Civile, Ordinanza 30 aprile 2012, n. 68/2011»: non posso essere sottoscritte con "un semplice clic", corrispondente alla firma elettronica, le clausole vessatorie di un contratto. Queste dovrebbero essere sottoscritte con firma digitale o autografa.

Siti web

- I siti web aziendali devono riportare in home page la partita IVA (DPR 633 del 1972, articolo 35).
- I siti web delle società iscritte nel registro delle imprese devono riportare: sede legale; ufficio del registro delle imprese presso il quale la società è iscritta; il numero d'iscrizione o la partita IVA; il capitale della società (somma effettivamente versata); se il socio è unico (articolo 2250 del Codice Civile, così come modificato dall'articolo 42 della Legge 88 del 2009).

Amministrazione digitale

Riferimenti normativi

- Il riferimento principale è il Dlgs 82 del 2005 (CAD).
  - Il Dlgs ha subito parecchi aggiornamenti, tutti oggetto di discussioni e critiche; gli ultimi dal Regolamento eIDAS (con Dlgs 179 del 2016).
  - La prima normativa sull'amministrazione digitale e in particolare delle "firme elettroniche" risale al 1997 (DPR 513), poi superata dal DPR 445 del 2000, ora parzialmente abrogato;
- Riferimenti tecnici sono emessi da AgID (www.agid.gov.it).
- Normativa tecnica specifica riguarda, tra gli altri:
  - conservazione dei documenti;
  - fatturazione elettronica;
  - giustizia digitale;
  - NUOVO SPID (che può essere usato anche per firmare, come da Regole AgID del 2020);
  - SPC (Sistema Pubblico di Connettività);
  - Posta elettronica certificata (PEC);
  - Firme elettroniche.
- Le aziende che offrono questi servizi devono adottare i requisiti tecnici (e in alcuni casi essere accreditati da AgID).

Firma digitale e documento informatico

- Il Dlgs 82 del 2005 definisce:
  - il documento informatico e analogico;
  - la firma elettronica avanzata e la firma elettronica qualificata (in eIDAS);
  - la firma digitale;
  - (insieme a eIDAS) come valutare la validità della firma e la copia dei documenti.
- Per SGQ-SGSI-ITSMS può essere utile verificare come le aziende gestiscono il/i dispositivo/i di firma.
- La normativa ha anche degli impatti sulla gestione documentale dei sistemi di gestione (ma non verrà trattato qui).

Posta Elettronica Certificata

- Tutte le imprese devono essere dotate di PEC per le comunicazioni con la PA o per altre comunicazioni.
- Potrebbe essere utile verificare come viene utilizzata (chi ne ha l'accesso, eccetera).
- Ricordare che la PEC è equivalente alla "raccomandata", non al documento firmato.
- DL 179 del 2012: "è facoltà di ogni cittadino indicare alla pubblica amministrazione un proprio indirizzo di posta elettronica certificata, quale suo domicilio digitale."

Conservazione delle registrazioni

- Articolo 2220 del Codice Civile “Conservazione delle scritture contabili”: “Le scritture devono essere conservate per dieci anni dalla data dell'ultima registrazione”

Infrastrutture critiche, NIS, perimetro di sicurezza e segreto di stato

Infrastrutture critiche

- Dlgs 61 del 2011: “Attuazione della Direttiva 2008/114/CE recante l'individuazione e la designazione delle infrastrutture critiche europee e la valutazione della necessità di migliorarne la protezione”.
- In base alla Direttiva, ogni azienda “critica” deve avere un responsabile della sicurezza unico, punto di contatto per tutte le questioni di sicurezza, e un “Piano della Sicurezza dell’Operatore”, con una dettagliata analisi delle minacce, vulnerabilità e, soprattutto, delle contromisure da adottare in funzione delle specifiche situazioni di rischio. Tutti gli oneri sono posti direttamente a carico delle aziende.
- Attualmente, le infrastrutture ICT non sono comprese dalla Direttiva, dedicata solo alle infrastrutture energetiche e dei trasporti.
  - Il D. Lgs. per essere attivo, prevede che siano elencate le aziende critiche.

NUOVO NOTA: questa normativa è non applicata, almeno ad oggi (gennaio 2020).

NUOVO Direttiva NIS

- Direttiva 2016/1148, detta NIS, del 6 luglio 2016, sulla sicurezza delle reti e dei sistemi informativi nell'Unione.
- Recepito in Italia con il D. Lgs. 65 del 2018.
  - Indirizzata agli "operatori di servizi essenziali (OSE) e dei fornitori di servizi digitali", con l'eccezione degli operatori di telecomunicazione (in quanto già normati dal Codice delle comunicazioni) e dei fornitori di servizi fiduciari (già normati da eIDAS e CAD), identificati entro il 9 novembre 2018 dalle "autorità competenti NIS".
  - Fornitori di servizi digitali ritenuti critici: Mercato online, Motore di ricerca online e Servizi di cloud computing (ad esclusione delle micro e piccole imprese).
  - Gli OSE dovranno comunicare alle autorità NIS le proprie misure di sicurezza (sono imposte le misure minime AgID).
  - Sono previsti audit da parte di «revisori abilitati».
  - Viene istituito il CSIRT italiano, unendo il CERT nazionale e il CERT-PA (il CERT-AgID sarà di tipo preventivo per la PA).
  - Molto spazio per richiedere di notificare gli incidenti.

NUOVO Perimetro di sicurezza nazionale cibernetica

- Normativa:
  - DL 105 del 2019 «Disposizioni urgenti in materia di perimetro di sicurezza nazionale cibernetica ((e di disciplina dei poteri speciali nei settori di rilevanza strategica))», convertito con Legge 133 del 2019;
  - DPCM 131 del 2020, "Regolamento in materia di perimetro di sicurezza nazionale cibernetica".
- Simile alla NIS: vanno identificate le entità che costituiscono il «Perimetro di sicurezza nazionale nel cyberspazio», esse dovranno attuare le Misure minime AgID, devono segnalare gli incidenti. Vanno anche comunicate "l'architettura e la componentistica relative ai beni ICT".
- Il DL stabilisce un centro di valutazione dei prodotti informatici (il Centro di Valutazione e Certificazione Nazionale, o CVCN, del MiSE), come peraltro già previsto, seppur parzialmente, dal Cybersecurity Act.
- Il DL dà la possibilità al Governo di spegnere una rete in caso di grave incidente.
- Purtroppo il termine "cibernetica" è usato a sproposito.

NUOVO

Cybersecurity Act

- Regolamento (UE) 2019/881 del Parlamento europeo e del Consiglio, del 17 aprile 2019, relativo all'ENISA, l'Agenzia dell'Unione europea per la cibersicurezza, e alla certificazione della cibersicurezza per le tecnologie dell'informazione e della comunicazione, e che abroga il regolamento (UE) n. 526/2013 («regolamento sulla cibersicurezza»).
- Concentrato sulla certificazione di sicurezza informatica di prodotti informatici (processi, prodotti e servizi TIC).
- ENISA dovrà promuovere gli schemi di certificazione, anche attraverso un sito web.
- Al momento sono in fase di studio alcuni schemi (p.e. Common Criteria o ISO/IEC 15408, IEC 62443, servizi cloud).

Segreto di Stato - Riferimenti normativi

- Il Segreto di Stato è regolamentato dalla Legge 124 del 2007 "Sistema di informazione per la sicurezza della Repubblica e nuova disciplina del segreto“, modificata nel 2012 dalla Legge 133/2012
- DPCM 22 luglio 2011 n.4 "Disposizioni per la tutela amministrativa del segreto di Stato e delle informazioni classificate"

Operatori di TLC e ISP

Normativa applicabile

- Il dispositivo di legge di riferimento per ISP e TLC è il Codice delle Comunicazioni Elettroniche (Legge Gasparri): Dlgs 259 del 2003.
- Altro dispositivo di interesse è il Dlgs 109 del 2008 sulla data retention.
- Le attività sono controllate dall'AGCOM (www.agcom.it).
- Ogni operatore deve redigere e pubblicare documenti sulla qualità dei servizi e la Carta dei Servizi per:
  - telefonia vocale fissa (Delibere n. 254/04/CSP e n. 79/09/CSP);
  - comunicazioni mobili e personali (Delibere n. 104/05/CSP e n. 79/09/CSP);
  - televisione a pagamento (Delibera n. 278/04/CSP);
  - accesso a Internet da postazione fissa (Delibere n. 131/06/CSP e n. 244/08/CSP).
- Non è più attivo il Decreto Pisanu per molti esercizi pubblici che mettono a disposizione le wi-fi (dovevano monitorare le operazioni degli utenti e identificarli).
- Le reti non devono più essere effettuate da imprese abilitate.
- Gli esercizi per i quali la connettività è "l'attività principale" devono disporre di licenza fornita dalla Questura.

Data retention

- Il Dlgs 109 del 2008 stabilisce gli obblighi di conservazione di log per gli operatori di TLC e ISP.
- L'elenco è lungo e riguarda sia comunicazioni telefoniche che elettroniche.
- Il Dlgs è stato molto criticato ed è di difficile applicazione.

Obblighi per gli operatori TLC

- Il Dlgs 109 del 2008 stabilisce gli obblighi di conservazione di log per gli operatori di TLC e ISP. questi log riguardano sia comunicazioni telefoniche che elettroniche.
- Dlgs 69/2012 con modifiche al Codice Privacy:
  - limitazione agli accessi del fornitore ai dati e ai dispositivi dei propri clienti;
  - richiesta di segnalare al Garante ogni violazione di dati personali;
  - richiesta di segnalare agli interessati ogni violazione di dati personali;
  - mantenzione di un registro delle violazioni di dati personali (i subfornitori comunicano al fornitore, non al Garante;
  - regolamentazione cookies.
- Dlgs 70/2012 con modifiche al Codice delle comunicazioni elettroniche:
  - misure di controllo del mercato, incluse richieste di interoperabilità;
  - specifiche misure di sicurezza (saranno stabilite dal Ministero dello sviluppo economico);
  - comunicazione al Ministero di violazioni della sicurezza;
  - creazione di un CERT nazionale.
- Provvedimento Garante 20 settembre 2012:
  - I requisiti del Capo 1 del Titolo X del Codice Privacy riguardano gli operatori di TLC e i loro abbonati (meglio: contraenti). Sono normati: la riservatezza dei dati dell'utente e gli apparati utilizzati, l'uso dei dati di traffico; la fatturazione di dettaglio; la visibilità o invisibilità del numero chiamante; i dati relativi all'ubicazione; il contrasto alle chiamate di disturbo; gli elenchi di abbonati.

Settore Finance

Basel, Solvency, eccetera

- Il settore finance è molto regolamentato. Tra le norme che possono avere impatto sulla sicurezza delle informazioni, ricordiamo:
  - Accordi di Basilea;
  - Direttive MIFID per gli operatori finanziari;
  - Direttiva Transparency (2004/109/CE) per gli operatori finanziari;
  - Direttiva sui servizi di pagamento (PSD2);
  - Direttiva Modernizzazione (direttiva 2003/51/CE);
  - Direttiva Solvency (2009/138/EC) per le assicurazioni.
- E anche:
  - (slide successiva)

Basel, Solvency, eccetera

- E anche:
  - regolamenti Banca d'Italia;
  - regolamenti ISVAP;
  - regolamenti dell'European Banking Authority (EBA)
  - regolamenti dell'European Payment Council (EPC).
- Particolare rilievo hanno
  - Istruzioni di Vigilanza di Banca d'Italia (http://www.bancaditalia.it);
  - Altre disposizioni di vigilanza; fondamentale la Circolare 285.

Sentenza su attacchi home banking

- Nel 2014 è stata emessa una sentenza intressante. Per il tribunale di Caltanisetta, il fatto che l'accesso all'home banking avvenga "solo" tramite user-id e password (nonostante comunque l'istituto bancario abbia sollecitato ai clienti l'adozione di un meccanismo di OTP), fa sì che un accesso abusivo al sistema sia da ritenere colpa dell'istituto bancario perché avrebbe potuto anche mettere a disposizione un servizio di SMS o simile.

Privacy

Riferimenti normativi

- I riferimenti sono:
- Regolamento (UE) 2016/679 (o GDPR);
- NUOVO il Regolamento 1807 del 2018 riguarda i dati non personali;
- il Dlgs 196 del 2003 (e successivi e numerosi aggiornamenti), aggiornato ad agosto 2018 con il D. Lgs. 101.
- Codici di condotta ancora in vigore.
- Sono importanti anche i Provvedimenti (norme e sentenze) del Garante:
  - Provvedimenti generali (es. su amministratori di sistema e videosorveglianza);
  - NUOVO Provvedimenti settoriali (banche, strutture sanitarie, eccetera).
- Ulteriori Direttive (2016/680 e 681) riguardano i dati usati per le indagini e il perseguimento di reati (recepiti con il Dlgs 51/2018).
- NOTA: Le norme italiane, se non sono in conflitto con il GDPR, sono applicabili.
- NOTA: Il GDPR non si applica al trattamento di dati personali effettuato da una persona fisica per l'esercizio di attività a carattere esclusivamente personale o domestico.

Definizioni dati personali

- **“Dato personale”:** qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato» o «data subject» o anche «PII principal»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale;
  - “interessato” è il termine italiano, “data subject” inglese, “PII principal” delle norme ISO/IEC.
- **“Dati personali appartenenti a categorie particolari (art. 9)”:** 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;
- **“Dati giudiziari” (“dati personali relativi a condanne penali e reati”):** dati personali relativi alle condanne penali e ai reati o a connesse misure di sicurezza.

Applicabilità all'estero

- La normativa si applica anche al trattamento di dati effettuato da chiunque è stabilito nel territorio di un Paese extra-UE e impiega, per il trattamento, strumenti situati nel territorio dello Stato. Il titolare del trattamento designa un proprio rappresentante stabilito nel territorio dello Stato.

NUOVO

- Per i trasferimenti extra-UE negli USA, è stato abrogato il protocollo "Safe Harbor" e anche il Privacy Shield. Sono quindi da usare le clausole contrattuali (e anche quelle pongono problemi).
- Per i trasferimenti extra-UE, vedere articoli 44-48 del GDPR. Previsti 3 meccanismi principali:
  - autorizzazioni della Commissione (oggi sono del Garante);
  - norme vincolanti di impresa per Gruppi o "Binding corporate rules (BCR)";
  - contratti (clausole, codice di condotta, certificazioni).

Soggetti

- Interessato (o “data subject”): la persona fisica cui si riferiscono i dati personali (non a persone giuridiche, enti o l'associazioni)
- "Titolare“ (o “controller”): la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali
- "Responsabile“ (o “processor”): la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento;
  - art. 28 del GDPR: Il responsabile del trattamento non ricorre a un altro responsabile senza previa autorizzazione scritta, specifica o generale, del titolare del trattamento;
- Persona fisica autorizzata a compiere operazioni di trattamento dal titolare o dal responsabile.

Informativa

- L'interessato o la persona presso la quale sono raccolti i dati personali sono previamente informati oralmente o per iscritto circa:
  - le finalità e le modalità del trattamento cui sono destinati i dati;
  - il periodo di conservazione dei dati
  - i soggetti o le categorie di soggetti ai quali i dati personali possono essere comunicati;
  - i propri diritti.
- Vedere l'Articolo 13 del GDPR.

Diritti dell'interessato

- I diritti dell'interessato sono elencati negli articoli dal 15 al 21 del GDPR:
  - Diritto di accesso;
  - Diritto di rettifica;
  - Diritto alla cancellazione ("diritto all'oblio");
  - Diritto di limitazione di trattamento;
  - Diritto alla portabilità dei dati;
  - Diritto di opposizione ("l'interessato ha il diritto di opporsi in qualsiasi momento al trattamento").

Consenso

- Il trattamento di dati personali da parte di privati o di enti pubblici economici è ammesso solo con il consenso espresso dell'interessato.
  - Il consenso può riguardare l'intero trattamento oppure una o più operazioni dello stesso.
  - Il titolare del trattamento deve essere in grado di dimostrare che l'interessato ha prestato il proprio consenso al trattamento dei propri dati personali.
  - La richiesta di consenso è presentata in modo chiaramente distinguibile dalle altre materie.
  - Il consenso è revocato con la stessa facilità con cui è accordato.
- Il consenso non è richiesto quando il trattamento:
  - è necessario per adempiere ad un obbligo previsto dalla legge, da un regolamento o dalla normativa comunitaria;
  - è necessario per eseguire obblighi derivanti da specifiche richieste dell'interessato (per esempio, anche un contratto o la gestione di un CV inviato spontaneamente);
  - rientra nelle casistiche dell'Articolo 9.
- NOTA: il GDPR non prevede più l'opt-out ("Registro delle opposizioni") per le attività di marketing (ma bisognerà vedere come sarà gestito il relativo Provvedimento).

Base giuridica per il trattamento

- I trattamenti di dati non appartenenti a categorie particolari possono essere effettuati sulla base di (art. 6):
  - consenso;
  - contratto;
  - obblighi legali (p.e. adempimenti contabili e amministrativi);
  - salvaguardia degli interessi vitali di persone;
  - interesse pubblico;
  - interessi legittimi del titolare (p.e. protezione aziendale, controllo della qualità).
- Per i dati appartenenti a categorie particolari, fare riferimento all'art. 9 del GDPR.
- Il trattamento di dati giudiziari è consentito solo previa autorizzazione normativa.

Notifica di violazioni ai dati personali

- Notifica al Garante (Articolo 33 del GDPR): In caso di violazione dei dati personali, il titolare del trattamento notifica la violazione all'autorità di controllo competente.
- Notifica all'interessato (Articolo 34 del GDPR): Quando la violazione dei dati personali è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento comunica la violazione all'interessato senza ingiustificato ritardo.

Codici di condotta e regole deontologiche NUOVO

- Codici di condotta (https://www.garanteprivacy.it/codici-di-condotta):
  - informazioni commerciali;
  - crediti al consumo, affidabilità e puntualità nei pagamenti.
- Regole deontologiche (https://www.garanteprivacy.it/codice). Quelle confermate nel 2019 sono quelle relative a:
  - attività giornalistica;
  - investigazioni difensive o per fare valere o difendere un diritto in sede giudiziaria;
  - scopi storici;
  - Sistema statistico nazionale;
  - scopi statistici e ricerca scientifica;
- Non sono più previste le autorizzazioni per il trattamento dei dati. Il Garante ha comunque fornitor (9124510) obblighi per il trattamento dei dati nei rapporti di lavoro e per scopi di ricerca scientifica e nel caso degli organismi di tipo associativo, delle fondazioni, delle chiese e associazioni o comunità religiose.

Altre misure importanti del GDPR (1/4)

- Protezione dei dati fin dalla progettazione ("**Privacy by design**") e protezione per impostazione predefinita ("**privacy by default**"):
  - articolo 25 del GDPR;
  - al momento di determinare i mezzi del trattamento sia all'atto del trattamento stesso il titolare del trattamento mette in atto misure tecniche e organizzative adeguate, quali la pseudonimizzazione, volte ad attuare in modo efficace i principi di protezione dei dati, quali la minimizzazione, e a integrare nel trattamento le necessarie garanzie al fine di soddisfare i requisiti del presente regolamento e tutelare i diritti degli interessati;
  - il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento.

Altre misure importanti del GDPR (2/4)

- **Registro dei trattamenti** per organizzazioni con più di 250 "dipendenti" (art. 30 del GDPR):
  - diverso per titolari e responsabili;
  - dati di contatto del titolare del trattamento;
  - finalità del trattamento;
  - categorie di interessati e delle categorie di dati personali;
  - categorie di destinatari a cui i dati personali sono stati o saranno comunicati;
  - trasferimenti di dati personali verso un paese terzo;
  - termini ultimi previsti per la cancellazione delle diverse categorie di dati;
  - una descrizione generale delle misure di sicurezza tecniche e organizzative.
- **Verifiche dell'efficacia** delle misure tecniche e organizzative (art. 32 dl GDPR).

Altre misure importanti del GDPR (3/4)

- Valutazione d'impatto sulla protezione dei dati o «**privacy impact assessment (PIA)**» (art. 35 del GDPR) quando il trattamento riguarda:
  - una valutazione sistematica e globale di aspetti personali relativi a persone fisiche, compresa la profilazione, e sulla quale si fondano decisioni che hanno effetti giuridici o incidono in modo analogo significativamente su dette persone fisiche;
  - il trattamento, su larga scala, di dati sensibili o giudiziari;
  - la sorveglianza sistematica su larga scala di una zona accessibile al pubblico;
  - pubblicata la WP 248 del WP Art. 29;
  - pubblicato tool del CNIL (anche in inglese).
- Il Garante:
  - dovrà rendere pubblico un elenco di trattamenti per cui è necessaria la PIA
  - potrà rendere pubblico un elenco di trattamenti per cui NON è necessaria la PIA.
- Se la PIA fornisce un livello di rischio molto elevato, il titolare deve consultare l'autorità di controllo prima di avviare il trattamento (art. 36 del GDPR).
  - Questo meccanismo sostituisce la "Notificazione al Garante" prevista dal D.Lgs. 196/2003;
  - eccezione sono i trattamenti «fondati sull'interesse legittimo che prevedono l'uso di nuove tecnologie o di strumenti automatizzati» per cui «darne tempestiva comunicazione al Garante per la protezione dei dati personali».

Altre misure importanti del GDPR (4/4)

- Responsabile della protezione dei dati o «**data protection officer (DPO)**» (art. 37-39 del GDPR):
  - obbligo in casi particolari, ma anche volontariamente;
  - il GDPR stabilise posizione e compiti del DPO;
  - pubblicata la wp 243 del WP Art. 29.
- **Certificazione** (facoltativa) su schemi o codici di condotta (art. 40-43 del GDPR);
  - le certificazioni professionali non sono "coperte" dal GDPR (ma in Italia è stata pubblicata la UNI 11697;
  - al momento non sono attive "certificazioni GDPR", approvate dal Garante.

Provvedimenti generali

- 23 novembre 2006: Linee guida in materia di trattamento di dati personali di lavoratori per finalità di gestione del rapporto di lavoro alle dipendenze di datori di lavoro privati.
- 1 marzo 2007: Utilizzo della posta elettronica e della rete Internet nel rapporto di lavoro.
- 13 ottobre 2008: Rifiuti di apparecchiature elettriche ed elettroniche (Raae) e misure di sicurezza dei dati personali.
- 27 novembre 2008: Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema (Importante l'aggiornamento del 25 giugno 2009 e le FAQ).
- 8 aprile 2010: Provvedimento su videosorveglianza (nel 2012 il Ministero del Lavoro ha semplificato alcune misure).
- Pagina dei provvedimenti generali: http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/3755203.
- Pagina delle linee guida: http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1772725.

Provvedimenti specifici

- Provvedimento sulle Carte Fedeltà (24 febbraio 2005).
- Provvedimento “Strutture sanitarie: rispetto della dignità” (9 novembre 2005).
- Provvedimento “Trattamento dei dati personali nell'ambito dei servizi telefonici non richiesti” (16 febbraio 2006).
- 15 giugno 2011: sentenza sul ruolo degli agenti (responsabili e non titolari).
- 12 maggio 2011: Prescrizioni in materia di circolazione delle informazioni in ambito bancario e di tracciamento delle operazioni bancarie.
- 5 maggio 2011: Linee guida in tema di trattamento di dati per lo svolgimento di indagini di customer satisfaction in ambito sanitario.
- 2 marzo 2011: Linee guida in materia di trattamento di dati personali contenuti anche in atti e documenti amministrativi, effettuato da soggetti pubblici per finalità di pubblicazione e diffusione sul web.
- Linee guida in materia di Dossier sanitario del 16 luglio 2009
- Regolamento in materia di fascicolo sanitario elettronico del 29/09/2015
- Regolamento “cookies” del 8 maggio 2014
- NOTA: è opportuno familiarizzare con il sito del Garante.

Spamming

- Decreto Ronchi, DL 135 del 2009 e convertito con Legge 166 del 2009:
  - D. Lgs. 196, Art. 130, comma 3-bis. Il trattamento dei dati mediante l'impiego del telefono e della posta cartacea per le finalità di invio di materiale pubblicitario o di vendita diretta o per il compimento di ricerche di mercato o di comunicazione commerciale è consentito nei confronti di chi non abbia esercitato il diritto di opposizione.
- Con il DPR 178 del 2010 è stato istituito il Registro delle Opposizioni (criticabile, per la verità);
  - applicabile anche alle imprese (Provvedimento del 20 settembre 2012).
- Con il DL 83/2012, l'utente deve essere avvisato sul Paese da cui ha origine la chiamata.
- Con il Dlgs 69/2012, si richiede che il mittente o il chiamante sia riconoscibile.
- Provvedimento 2013 sui Call center extra-UE (applicabile a tutti i soggetti che svolgono in qualità di titolare del trattamento un'attività di call center in maniera prevalente): i call center devono dichiarare la nazione dalla quale chiamano o rispondono; per le chiamate in entrata, dovrà essere data all'utente la possibilità di scegliere un operatore collocato sul territorio nazionale; dovrà essere segnalato preventivamente al Garante l'affidamento delle attività di call center in Paesi extra-UE.
- NUOVO Legge 5 del 2018 (ma manca il decreto di attuazione!):
  - obbligo di rendere identificabile la linea chiamante per scopi commerciali o statistici;
  - inclusione nel registro delle opposizioni dei numeri mobili.

NUOVO Piccolo spazio pubblicità

- Il ricavato andrà in beneficenza.

Sicurezza fisica

Riferimenti Normativi

- La 626 del 1994 è stata abrogata nel 2008 e vige il Dlgs 81 del 2008.
- Il Dlgs 81 è stato modificato nel 2009 con il Dlgs 106.
- I seguenti punti sono di interesse per la sicurezza delle informazioni:
  - inserire a organigramma il Responsabile Sicurezza;
  - eventuali impatti dell'analisi dei rischi ex-81 con quella ex-27001 (e quella ex-196);
  - identificazione del personale esterno all'interno della struttura;
  - presenza, correttezza (senza pericolo per vite umane e ben segnalato) e manutenzione (almeno ogni 6 mesi) dell'impianto anti-incendio;
  - presenza del Certificato Prevenzione Incendi valido.
- Se non si è esperti di sicurezza dei lavoratori, è preferibile interfacciarsi con il referente aziendale sulle materie sopra indicate.

Prodotti sicuri

- I prodotti elettrici ed elettronici devono essere sicuri. In particolare, devono essere conformi a:
  - Direttiva 2014/30/UE (Dlgs 80/2016 e Dlgs 194/2007) su EMC;
  - Direttiva 2014/35/UE (Dlgs 86 del 2016) su bassa tensione (BT);
  - Direttiva 2014/53/UE (Dlgs 128 del 2016) su apparecchi radio e tlc (RTTE);
  - Direttiva 1999/5/CE (Dlgs 269/2001) su apparecchiature terminali di telecomunicazione;
  - Direttiva 2011/65/EEC (Dlgs 251 del 2005), con aggiornamento 2015 su RHOS;
  - Direttiva 2014/32/UE (Dlgs 22 del 2007) su strumenti di misura (MID);
- Se acquistati da un distributore in territorio UE, entro certi limiti, non è responsabilità dell'utilizzatore la valutazione della conformità.
- Dal 2013, le reti informatiche non devono più essere realizzate da imprese abilitate. Attenzione però che le reti di telecomunicazione devono rispondere ai requisiti di sicurezza degli impianti stabiliti dalla Legge 46 del 1990.

Transizione delle Direttive del 2014

Nel periodo transitorio i nuovi prodotti dovranno essere conformi alla nuova direttiva, quelli che erano in commercio e conformi alla precedente direttiva si potranno continuare a vendere fino al 20/4/2016. Dopo tale data le dichiarazioni di conformità dovranno essere aggiornate.

Prodotti sicuri – norme ISO

- Per alcuni prodotti specifici sono presenti delle norme ISO relativamente alla loro affidabilità (non dedicate alla sicurezza rispetto ad attacchi di malintenzionati).
- Tra di essi:
  - ISO 26262-xx:2012 (dove xx va da 01 a 10, visto che la norma è divisa in 10 parti): Road vehicles - Functional safety

Varie normative

Telelavoro e reperibilità

- Il telelavoro è regolamentato dall'accordo interconfederale del 9 giugno 2004:
  - Articolo 2: il datore di lavoro provvede a fornire al telelavoratore le relative informazioni scritte.
  - Articolo 4 - Protezione dei dati: Il datore di lavoro ha la responsabilità di adottare misure appropriate, in particolare per quel che riguarda il software, atte a garantire la protezione dei dati utilizzati ed elaborati dal telelavoratore per fini professionali.
  - Articolo 6 - Strumenti di lavoro: Di regola, il datore di lavoro è responsabile della fornitura, dell'istallazione e della manutenzione degli strumenti necessari ad un telelavoro svolto regolarmente, salvo che il telelavoratore non faccia uso di strumenti propri; in caso di guasto o malfunzionamento degli strumenti di lavoro il telelavoratore dovrà darne immediato avviso alle strutture aziendali competenti.
- Parte di queste misure dovrebbero essere considerate applicabili anche a chi lavora in reperibilità (anche se questo non è previsto dall'accordo, ma deve essere previsto caso per caso).

Vigilanza

- È di interesse per la sicurezza delle informazioni anche il decreto 115/2014 applicabile agli istituti di vigilanza privati.
- Essi, per poter operare, devono obbligatoriamente ottenere il certificato di conformità dei propri servizi, impianti e professionisti secondo le norme UNI 10891 (istituti di vigilanza privata); UNI 50518 (centri di monitoraggio) e 10459 (professionista della security), da parte di un organismo di certificazione accreditato da un Ente designato, quale Accredia in Italia.

Per finire

Qualche spunto

- Ogni norma va “interpretata”, anche a fronte di pareri, discussioni e sentenze.
- Gli uffici legali di un’impresa ne sanno spesso di più; se non lo sanno, sono comunque loro che devono gestire le cose (in altre parole: non fare gli ignoranti, ma non fare i saccenti).
- Bisogna tenersi aggiornati.

Per aggiornarsi

- Newsletter Cesare Gallotti (mensile).
- www.normattiva.it: per avere i testi aggiornati.
- Newsletter Filodiritto: www.filodiritto.com.
- Newsletter Altalex: www.altalex.com.
- Garante Privacy (con newsletter): www.garanteprivacy.it.
- Europrivacy: http://www.europrivacy.info.

www.dnvgl.com

SAFER, SMARTER, GREENER