LA COSTRUZIONE DEL DOMICILIO INFORMATICO AZIENDALE

DAL MOBILE AI PENETRATION TEST

Avv. Andrea Nicolò Stanchi

StanchiStudioLegale

a.stanchi@stanchilaw.it

FATTISPECIE ILLECITE

- Art. 392 c.p.
- Art. 615 ter c.p.
- Art. 615 quater c.p.
- Art. 615 quinquies c.p.
- Art. 617 quater c.p.
- Art. 617 quinquies c.p.
- Art. 617 sexies c.p.
- Art. 635 bis c.p.
- Art. 640 ter c.p.
- Il Phishing
- Art. 171 bis L.d.A.
- Il file sharing
- Pubblicazione di immagini e musica in rete
- Altre sanzioni a tutela del software
- Pornografia minorile
- Illeciti penali nel Cod.Privacy

NORMATIVA DI RIFERIMENTO

1. L. n. 547 del 1993;
2. L. n. 48 del 2008 (ratifica Convenzione di Budapest sui crimini informatici)
3 D.lgs. 231/01 art. 24 ssg.

Tecnica legislativa particolare:

- Introduzione di nuove fattispecie criminose nel codice penale
- Modifica articoli del codice penale preesistenti

CONDOTTE ILLECITE

Occorre distinguere tra:

- Fatti illeciti commessi sul sistema (il sistema rappresenta l'oggetto del reato);
- Fatti illeciti commessi attraverso il sistema (il sistema è mezzo del reato).

IL DOMICILIO VIRTUALE

sistemi informatici e telematici

Ampliamento dell’area pertinente al soggetto interessato, garantita dall’articolo 14 Cost. e penalmente tutelata nei suoi aspetti essenziali.

TUTELA DEL “DOMICILIO INFORMATICO”

art.4 L. 547/93

- introduce nel codice penale gli artt. 615 *ter*, *quater*, *quinquies* (nell’ambito dei delitti contro l’inviolabilità del domicilio)
- sistemi informatici/telematici non solo come strumenti per compiere l’illecito penale, ma anche come luogo ove l’uomo trasferisce alcune delle proprie facoltà intellettuali

DOMICILIO INFORMATICO

"*non solo è il luogo ove il soggetto avente diritto può esplicare liberamente qualsiasi attività lecita, ma è un'area la cui tutela, grazie all'art. 615 c.p. si estende anche nello ius excludendi alios*"

(Cass.Pen. n. 3097/1999)

ACCESSO ABUSIVO SISTEMA INFORMATICO O TELEMATICO (ART. 615 *TER* C.P.)

"Chiunque abusivamente (1) si introduce in un sistema informatico o telematico protetto da misure di sicurezza ovvero (2) vi si mantiene contro la volontà espressa o tacita di chi ha il diritto di escluderlo, è punito con la reclusione fino a tre anni"

NATURA

- È un reato di pericolo:

  rischio che chi accede abusivamente a un sistema sia in grado di impadronirsi o conoscere quanto custodito in esso.
- Si consuma con:

  intrusione in quanto tale (non rileva apprensione del contenuto delle informazioni contenute nel sistema o il successivo intervento dannoso sul sistema).

REQUISITI

- ✓ È necessario che il sistema sia stato protetto da misure (minime) di sicurezza, tali da offrire un impedimento;
- ✓ la presenza di un sistema di sicurezza è sufficiente ad evidenziare la volontà del titolare del diritto, di escludere chi da lui non autorizzato ad accedere al sistema.

CASSAZIONE PENALE N. 12372 DEL 2000

- non occorre che le misure di sicurezza siano costituite da chiavi d'accesso o altre analoghe protezioni (protezione interna);
- è sufficiente qualsiasi meccanismo di selezione dei soggetti abilitati all'accesso, anche quando si tratti di strumenti esterni al sistema e meramente organizzativi, in quanto destinati a regolare l'ingresso stesso nei locali in cui gli impianti sono custoditi.

RATIO DELLA DECISIONE

l'art. 615 ter c.p. non punisce solo chi abusivamente si introduce in un sistema protetto ma anche chi vi si **mantiene** contro la volontà espressa o tacita di chi il diritto di escluderlo.

"*contravvenzione alle disposizioni del titolare*"

Volontà (anche implicita) del titolare di disporre autonomamente e liberamente dell'unità di elaborazione, escludendo o limitando gli accessi alle persone legittimate

Mantiene: Indica il "*persistere nella già avvenuta introduzione, inizialmente autorizzata o casuale, violando le disposizioni, i limiti e i divieti posti dal titolare del sistema*"

Cass. SS.UU., sent. 17325/2015

STANCHI
STUDIO LEGALE

RATIO DELLA DECISIONE (AMBITO)

II

- "**non esce** dall'area di applicazione della norma l'abuso delle proprie funzioni (accesso o mantenimento con credenziali **proprie dell'agente P.U. ed in assenza di espressi divieti** ma con sviamento di potere: un uso del potere in violazione dei doveri di fedeltà connessi agli specifici compiti assegnati e in diretta connessione con l'assolvimento della propria funzione)
  Cass. SS.UU., sent. 41210/2017
- la **conoscenza della password** di accesso **non esclude** il carattere abusivo degli accessi, in considerazione del risultato ottenuto - **palesemente in contrasto con la volontà del titolare della casella elettronica** - di determinare "il cambio della password con impostazione di una nuova domanda di recupero ed inserimento della frase" ingiuriosa "quando lo hai preso nel k…"..." Cass. Sez. V, sent 52572/2017
- Nel caso di dipendenti che accedono al sistema aziendale per sottrarre i codici sorgente dei programmi (e successivamente realizzare un programma analogo) sussiste l'illiceità penale della condotta consistente in **un ingresso nel sistema telematico con fini palesemente contrari agli interessi – anche patrimoniali - del titolare del sistema informatico stesso**
  Cass. Sez. 2 sent. 11075/2018

STANCHI
STUDIO LEGALE

PER QUANTO CI INTERESSA…

misura di sicurezza rilevante per art. 615-*ter* c.p. (e quindi protezione domicilio)

a. qualunque meccanismo idoneo a far trasparire la volontà (anche implicita) di escludere;

b. presenza di un'obiettiva protezione del sistema.

CIRCOSTANZA AGGRAVANTE

operatore di sistema

1. operatore in senso stretto: addetto alle operazioni di input e output, di avviamento o di arresto del sistema;
2. programmatore: scrive, con appositi linguaggi, le operazioni che il computer sarà chiamato ad effettuare;
3. sistemista: studia le possibili evoluzioni di un sistema per ottimizzarlo e implementarlo;
4. analista: scopre o inventa gli algoritmi

DETENZIONE E DIFFUSIONE ABUSIVA DI CODICI DI ACCESSO A SISTEMI INFORMATICI E TELEMATICI (ART. 615-*QUATER* C.P.)

"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 fino ad un anno e con la multa fino a euro 5.164,00"*.

presupposto

il sistema informatico/telematico deve essere protetto da misure di sicurezza

NUOVO ART. 615-*QUINQUIES* CP

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 funzonamento, 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 10.3292*

1. Dolo specifico
2. Condotte tipizzate

STANCHI
STUDIO LEGALE

DANNEGGIAMENTO DI SISTEMI INFORMATICI (ART. 635-*BIS* C.P.)

Salvo che il fatto costituisca più grave reato, 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*

- **Punibilità a querela della persona offesa**
- **Chi è la persona offesa dal reato (rilevanza policy)?**

1. interessato, titolare e responsabile del trattamento/sistema;
2. concessionario, utilizzatore, concedente, proprietario del programma
3. Partners commerciali o di lavoro

STANCHI STUDIO LEGALE

ARTT. 635-*TER*, *QUATER*, *QUINQUIES* CP

La L. n. 48 del 2008 introduce:

1. art. 635-*ter* cp (danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità)
2. art. 635-*quater* cp (danneggiamento di sistemi informatici o telematici)
3. art. 635-quinquies cp (danneggiamento di sistemi informatici o telematici di pubblica utilità)

FRODE INFORMATICA (ART. 640-TER C.P.)

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 se 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 516 a euro 1032. La pena è della reclusione da uno a cinque anni e della multa da euro 309 a euro 1549 se ricorre una delle circostanze previste dal n.1 del secondo comma dell'art. 640 ovvero se il fatto è commesso con abuso della qualità di operatore del sistema […]*

CONDOTTE ILLECITE

- alterazione in qualunque modo del funzionamento di un sistema informatico/telematico, procurando a sé o ad altri un ingiusto profitto con danno per il soggetto passivo;
- intervento **senza diritto** in qualunque modo su dati, informazioni o programmi contenuti in un sistema informatico/telematico, procurando a sé o ad altri un ingiusto profitto con danno altrui

STANCHI
STUDIO LEGALE

PRIVACY, SISTEMI AZIENDALI E 4.0

- Il principale impatto che la utilizzazione di tecnologie 4.0 e delle sue applicazioni ha avuto sulla privacy è il forte legame con la sicurezza degli apparati informatici;
- La sicurezza informatica, cioè la tutela dei sistemi da potenziali rischi e/o violazioni dei dati custoditi negli archivi digitali è diventata la condizione necessaria per la protezione della privacy.
- La controllabilità della sicurezza del sistema passa dal bilanciamento della propria area di rispetto da quella della privacy altrui: essenzialità della definizione del domicilio informatico.

COSA DEVE GARANTIRE LA SICUREZZA

- La RISERVATEZZA dei dati (cioè la riduzione del rischio che si possa accedere alle informazioni senza autorizzazione)
- L'INTEGRITA' dei dati (cioè la riduzione del rischio che possano essere modificati i cancellati da chi non è autorizzato)
- La DISPONIBILITA' (cioè la riduzione del rischio che non si possa accedere alle info a causa di interventi di terzi)

ACCOUNTABILITY

Approccio basato sulla valutazione del rischio che premia i soggetti più responsabili

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. 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».

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

SICUREZZA DEI SISTEMI

- rispetto dei principi, **privacy by design/default**
- **di avere effettuato, nei casi previsti, la valutazione di impatto**
- **di avere adottato delle procedure di sicurezza**
- **di avere effettuato la valutazione dei rischi**
- **la tenuta e registro dei trattamenti**
- **gestione dei data breach**
- **sistema di audit**

(ART. 32) RGDP

1. Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, 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, se del caso:

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 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) una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

PROVVEDIMENTO SU DATA BREACH 21 DICEMBRE 2017

- A. I futuri sviluppi dovranno sempre essere validati sul piano della sicurezza informatica da adeguate azioni di **vulnerability assessment** attuate precedentemente alla messa in esercizio, allo scopo di individuare e correggere eventuali vulnerabilità nei servizi prima di renderli fruibili al pubblico. Le verifiche sulla tenuta delle misure di sicurezza dovranno essere periodicamente rinnovate, al fine di garantire un livello costante nel tempo di protezione dei dati personali.
- B. Con riferimento al **sistema di autenticazione informatica** degli utenti, lo stesso dovrà essere modificato in modo che le password relative alle utenze siano di lunghezza non inferiore a otto caratteri e siano sottoposte a un controllo automatico di qualità che impedisca l'uso di password "deboli" costituite, ad esempio, da parole reperibili in dizionari o comunque facilmente individuabili. Contestualmente devono essere introdotte strette limitazioni al numero di tentativi di accesso online con password erronea, per impedire attacchi brute force interattivi.

SEGUE …

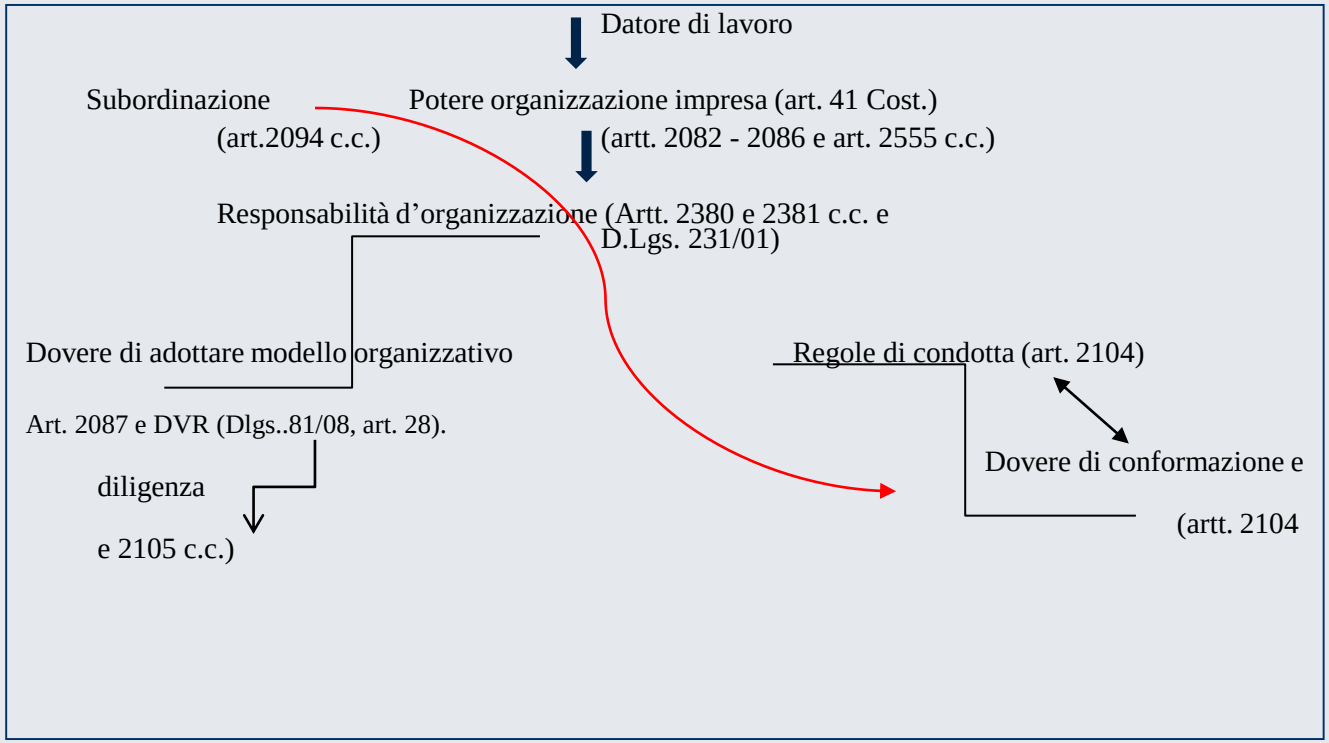
- C. Con riferimento ai **protocolli di rete**, si ritiene necessario prescrivere l'adozione del protocollo https (secure hyper text transport protocol) per l'accesso a tutti i contenuti del, basato su un certificato digitale emesso da una Certification Authority riconosciuta,
- D. Con riferimento al **database delle utenze** , si ritiene necessario prescrivere che le modalità di conservazione delle password degli utenti siano rafforzate adoperando algoritmi crittografici robusti in luogo delle semplici routine di cifratura accessibili tramite le funzioni native del CMS medesimo.
- E. Con riferimento alle **misure di auditing** per la verifica della liceità dei trattamenti compiuti dagli incaricati dotati di profili di autorizzazione ampi e speciali, allo scopo di fornire maggiori garanzie a tutela si ritiene necessario prescrivere l'adozione di misure che consentano l'auditing informatico mediante la tenuta delle registrazioni degli accessi e delle operazioni compiute (log) sul database del sistema, attuando gli accorgimenti di cui al provvedimento generale del Garante del 27 novembre 2008 in tema di amministratori di sistema (doc. web **1577499**)

GLI ASSESSMENT AVANZATI DI SICUREZZA.

Red Teaming:

- Nel settore della sicurezza informatica si tratta di esperti che proveranno a colpire il cliente oggetto di test nei seguenti ambiti:
  - Tecnologico: violazione del perimetro, dei servizi esposti, applicazioni *web*, *router*, *appliances*
  - Umano: *social engineering* contro lo staff
  - Fisico: accesso a edifici o proprietà aziendali
- In termini tecnici, questa attività ha aspetti comuni ai **Penetration tests**, ma si tratta di due tipologie di assessment totalmente differenti:
  - Il Penetration Testing ha lo scopo di individuare e validare il maggior numero di vulnerabilità presenti sui sistemi di un'azienda. Non fornisce alcun tipo di indicazione rispetto a quali potrebbero essere le azioni intraprese da un reale attaccante.
  - Il Red Team ha lo scopo di fornire una fotografia del livello di rischio reale a cui un Ente è soggetto.

IL DATORE DI LAVORO COME ORGANIZZAZIONE



QUALI NORME ALLORA REGOLANO LA PRIVACY NEL RAPPORTO DI LAVORO?

L'unica opinione coerente, basata in particolare sulle precisazioni dell'art.2 e sgg. nel testo novellato dal Lgs. 101/18 è che la privacy è normativa generale ma lo Statuto dei Lavoratori, in quanto normativa di settore, integra i principio della «base giuridica» del trattamento.

Va rispettata la normativa privacy e vanno rispettate le regole specifiche dello Statuto.

SEGUE

Anche dopo il GDPR restano validi i provvedimenti già adottati dal Garante. In particolare:

- Provvedimento 9 marzo 2005, linee guida per l'Uso degli RFID.
- Provvedimento 23 novembre 2006, sul trattamento dei dati dipendenti privati, con le opportune armonizzazioni (cfr. anche GP21.4.11n.89)
- Provvedimento 1 marzo 2007: Linee guida per l'utilizzo della posta elettronica e internet.
- Provvedimento 8 aprile 2010: trattamento dei dati personali effettuato tramite sistemi di videosorveglianza.
- Provvedimento 4 ottobre 2011: sistemi di localizzazione dei veicoli nell'ambito del rapporto di lavoro.
- Provvedimento 12 novembre 2014: biometria.
- Provvedimento 1 febbraio 2018: Trattamento di dati personali effettuato sugli account di posta elettronica aziendale che richiama espressamente il secondo.
- Permane l'efficacia interpretativa delle Opinion del DPWP ex art. 29 della Direttiva.

L'AMBIENTE DIGITALE AZIENDALE – ART. 4 SL (NOVELLATO DA D.LGS.151/15)

- *Gli impianti audiovisivi e gli altri strumenti dai quali derivi anche la possibilità di controllo a distanza dell'attività dei lavoratori impiegati per esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio aziendale;*
- *strumenti utilizzati dal lavoratore per rendere la prestazione lavorativa e agli strumenti di registrazione degli accessi e delle presenze.*

LE REGOLE DELLA SICUREZZA TU 81/08

- *"a tutti i lavoratori subordinati che effettuano una **prestazione continuativa** di lavoro a distanza, mediante collegamento informatico e telematico … si applicano le disposizioni di cui al titolo III* (ndr. Dispositivi di protezione individuale: artt. 69-87; e specie capo III) *e VII* (ndr. Artt. 172-179, disposizioni per i videoterminali) *del citato decreto, indipendentemente dall'ambito in cui si svolge la prestazione stessa"* (art. 3, co. 10 D.Lgs. 81/08)
  - Telelavoro: Disposizioni dell'Allegato XXXIV.
- Risk assessment.
  - Stress (art. 28, co.1, D:lgs. 81/80):
    - Ergonomia del software (punto 3, All. XXXIV);
    - Divieto di controlli qualitativi/quantitativi occulti.
    - Fenomeno della "Colonizzazione della notte"
- Diritto di accesso del datore di lavoro.

LE REGOLE DELLA SICUREZZA TU 81/08 - SEGUE

- il posto di lavoro comprende videoterminali, tastiera, mouse software per l'interfaccia uomo-macchina, gli accessori opzionali le apparecchiature connesse comprese unità dischi, telefono modem stampante …. (art. 173 Testo Unico 81/08).

CASS.SEZ.V PEN. 13057/16.

- Un sistema informatico è il complesso organico di elementi fisici (Hardware) e astratti (software) che compongono un apparato di elaborazione dati;
- Casella posta è uno spazio di memoria del sistema destinato a memorizzare messaggi o informazioni di un soggetto identificato da un account registrato presso un provider di servizio;
- L'apposizione di PWD dimostra esclusività (domicilio informatico ai sensi 615ter cp)
- Le caselle dei dipendenti della PA sono domicilio dei medesimi (ius excludendi alios);
- Anche il superiore pertanto è estraneo e deve tenerne conto.

LA POSIZIONE DEL GARANTE PRIVACY SUGLI STRUMENTI DI LAVORO

- *In tale nozione, infatti - e con riferimento agli strumenti oggetto del presente provvedimento, vale a dire servizio di posta elettronica e navigazione web - è da ritenere che possano ricomprendersi solo servizi, software o applicativi strettamente funzionali alla prestazione lavorativa, anche sotto il profilo della sicurezza.*
- **[GP. doc. web n. 5408460, 13 luglio 2016]**

LINEE GUIDA ALLE ISTITUZIONI UE 17 DICEMBRE 2015, GARANTE EUROPEO DELLA PROTEZIONE DEI DATI (EDPS) AI SENSI DIRETTIVA 45/2001 SUI MOBILE E BYOD

- **Informativa**

L'utilizzo dei device sul luogo di lavoro comporta il trattamento dei dati personali nello stesso riportati che, naturalmente, deve essere ben specificato in apposita informativa. Tale informativa deve essere rilasciata dal datore di lavoro ad ogni singolo dipendente che usa il device in qualità di interessato e nella stessa devono essere chiaramente riportate le seguenti informazioni:

- chi è il titolare dei dati trattati e quali sono i dati trattati;
- quali sono i dati personali che l'utente può raccogliere ed elaborare tramite il dispositivo;
- quali applicazioni sono autorizzate e possono essere scaricate sul dispositivo;
- qual è la politica per quanto riguarda l'uso dei servizi cloud;
- qual è la politica relativa alla dismissione del dispositivo ed allo smaltimento dello stesso;
- una chiara descrizione delle responsabilità dell'utente e della istituzione dell'UE;
- come si atteggia il monitoraggio dell'uso di dispositivi mobili da parte del personale; etc.

APPLICATIVI DI PROFILAZIONE

- (considerando 71) L'interessato dovrebbe avere il diritto di non essere sottoposto a una decisione, che possa includere una misura, che valuti aspetti personali che lo riguardano, che sia basata unicamente su un trattamento automatizzato e che produca effetti giuridici che lo riguardano o incida in modo analogo significativamente sulla sua persona, quali il rifiuto automatico di una domanda di credito online o **pratiche di assunzione elettronica** senza interventi umani. Tale trattamento comprende la «profilazione», che consiste in una forma di trattamento automatizzato dei dati personali che valuta aspetti personali concernenti una persona fisica, in particolare al fine di analizzare o prevedere aspetti riguardanti **il rendimento professionale**, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti dell'interessato, ove ciò produca effetti giuridici che la riguardano o incida in modo analogo significativamente sulla sua persona.

ART. 4 RGDP

- 4) «profilazione»: qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti **il rendimento professionale**, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica; (C24, C30, C71-C72)

ART. 13 E 14

- (13) f) l'esistenza di un processo decisionale automatizzato, compresa la profilazione di cui all'articolo 22, paragrafi 1 e 4, e, almeno in tali casi, **informazioni significative sulla logica utilizzata**, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato.
- (14) g) l'esistenza di un processo decisionale automatizzato, compresa la profilazione di cui all'articolo 22, paragrafi 1 e 4, e, almeno in tali casi, **informazioni significative sulla logica utilizzata**, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato.

ALLEGATO 1 AL PROVVEDIMENTO N. 467 DELL'11 OTTOBRE 2018 [DOC. WEB N. 9058979] TRATTAMENTI CHE RICHIEDONO DPIA

- Trattamenti valutativi o di scoring su larga scala, nonché trattamenti che comportano la profilazione degli interessati nonché lo svolgimento di attività predittive effettuate anche on-line o attraverso app, relativi ad "aspetti riguardanti il **rendimento professionale**, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti dell'interessato".
- Trattamenti effettuati nell'ambito del rapporto di lavoro mediante sistemi tecnologici (anche con riguardo ai sistemi di videosorveglianza e di geolocalizzazione) dai quali derivi la possibilità di **effettuare un controllo a distanza** dell'attività dei dipendenti (si veda quanto stabilito dal WP 248, rev. 01, in relazione ai criteri nn. 3, 7 e 8).
- Trattamenti effettuati attraverso **l'uso di tecnologie innovative, anche con particolari misure di carattere organizzativo** (es. IoT; sistemi di intelligenza artificiale; utilizzo di assistenti vocali on-line attraverso lo scanning vocale e testuale; **monitoraggi effettuati da dispositivi wearable; tracciamenti di prossimità come ad es. il wi-fi tracking**) ogniqualvolta ricorra anche almeno un altro dei criteri individuati nel WP 248, rev. 01
- Trattamenti sistematici **di dati biometrici**, tenendo conto, in particolare, del volume dei dati, della durata, ovvero della persistenza, dell'attività di trattamento.

CEDU 5 SETTEMBRE 2017 B VS. ROMANIA

- 140. In tale contesto, sembra che i tribunali interni **non abbiano determinato**, in particolare, se il ricorrente fosse stato preliminarmente informato dal datore di lavoro della possibilità che le comunicazioni che effettuava mediante Yahoo Messenger avrebbero potuto essere monitorate; né hanno tenuto conto del fatto che non fosse stato informato **del carattere o della portata del monitoraggio o del livello di invasività** nella sua vita privata e nella sua corrispondenza. Non hanno inoltre determinato, in primo luogo**, i motivi specifici** che giustificavano l'introduzione delle misure di monitoraggio; in secondo luogo, la questione di sapere se il datore di lavoro **avrebbe potuto utilizzare misure che comportavano una minore invasione nella vita privat**a e nella corrispondenza del ricorrente; in terzo luogo, se sarebbe stato possibile **accedere alle comunicazioni a sua insaputa** (si vedano i paragrafi 120 e 121 supra).

QUINDI COSA SIGNIFICA FARE UNA POLICY?

- Classificare i dati
- Stabilire procedure di verifica (degli accessi) e autorizzazione (strutture privacy incarichi);
- Stabilire procedure gestionali (dati, ingressi, telefoni, badge; account fornitori, hot line incidenti, account clienti provider servizi, test di vulnerabilità periodici, training; audit);
- Politiche sulla IT (riservatezza numeri dip IT, assistenza tecnica, help desk, password, privilegi accesso, blocco porte seriali, amministrazione pc, configurazioni di sistemi, gestione siti web accessibili, guest account, codifica Back up esterni, autentica sw, VPN, Antivirus, regole monitoraggi)
- Stabilire politiche per tutto il personale (report anomalie, badge classificati, divieto accessi non registrati, distruzione documenti, identificatori personali, organigrammi, obbligo segnalazione a HR di richieste info sui dipendenti, regole uso PC e SW, supporti esterni, Salvaschermo con pwd, regole per email, telefoni, mobile, politiche specifiche per il telelavoro);
- Stabilire politiche specifiche per le HR (regole assunzioni, verifiche preassuntive, gestione valutazione prestazioni, chiusura account dimessi/licenziati; notifiche settore IT delle modifiche; rigorosa riservatezza sui dai personali dipendenti, back checks)
- Stabilire politiche di sicurezza fisica (badge esterni, scortare esterni, aree di accesso contingentate, regole per portieri, regole per gestione incidenti).

CONCLUDENDO

- Cambia il livello di valutazione della integrazione tra le tecnologie aziendali;
- La definizione del domicilio informatico aziendale diviene essenziale e le scelte vanno ponderate con consapevolezza dei limiti che comportano;
- L'integrazione tra misure organizzative, fisiche, logiche muta la pratica organizzativa;
- La logica informativa diviene molto più specifica e penetrante di quella ammessa dalle linee guida generali.

Grazie dell’attenzione

Avv. Andrea Stanchi

a.stanchi@stanchilaw.it
www.stanchilaw.it

STANCHI STUDIOLEGALE