OCCASIONAL PAPERS

RIFLESSIONI **N. 4**

Privacy, protezione dati e impresa

La nuova disciplina in un sistema *"globale"*

Franco Pontani

Privacy, protezione dati e impresa

La nuova disciplina in un sistema *"globale"*

Franco Pontani

Scenari di cambiamento

Viviamo in un'epoca di grandi cambiamenti e l'accelerazione dell'evoluzione tecnologica è tale che non sempre le imprese riescono a coglierne la portata globale, ma ne considerano solo gli effetti immediati considerati in un'ottica strettamente utilitaristica.

In altre parole l'impresa non coglie se non marginalmente l'impatto che tali mutamenti sistemici avranno sulla sua architettura. Lo *tsunami* è all'orizzonte e non si valuta in modo corretto la sua portata ed il tempo occorrente per il suo arrivo alla costa (la nostra impresa).

Siamo in presenza del rischio *"Fukushima 2.0"*, ma pensiamo di esserne al riparo, e se le nostre dighe reggeranno all'impatto, ne governeremo le conseguenze.

L'impatto è globale e non locale e, realisticamente, molte sono le imprese sprovviste di adeguate tutele, moltissime quelle che non sono, allo stato, in grado di affrontare in modo adeguato i mutamenti generati dalle *disrupting technologies* e le connesse conseguenze economiche e giuridiche.

In questo modo (carente) si è, d'altronde, considerata la crisi sistemica della finanza nel suo mondo globalizzato e, alla fine, si è detto e scritto che la crisi ha reso evidenti le carenze dei sistemi di controllo preesistenti, ma confusamente adattati alle circostanze con l'effetto di incremento dei fallimenti, disoccupazione, suicidi.

La società dell'informazione, della comunicazione ed il mondo digitale

Viviamo in quello che è stato denominato *"digital world"* in quella che è stata qualificata come l'*"era dell'informazione e della comunicazione"* (non solo meramente sociale) ed in detta *"era"*, la non conoscenza o l'inadeguata (in relazione ai ruoli ed alle funzioni da espletare) conoscenza, per quanto possa essere compatibile con una situazione originaria, una condizione iniziale, in presenza di consapevolezza il difetto conoscitivo diviene una scelta e se detta scelta conduce ad un danno per altri allora diviene una colpa.

Naturalmente, per ogni individuo ed ogni organizzazione esiste sempre uno stato di inadeguata conoscenza di aree, materie, situazioni, ma tale *"difetto"* deve essere *"contenuto"* nei limiti della ragionevolezza, in relazione alle singole circostanze, e in osservanza del principio che il proprio comportamento deve essere sempre governato dalla (ragionevole) prudenza (e da un naturale scetticismo rigettando la consueta giustificazione *"si è sempre fatto così"* o *"così fanno tutti"* ovvero *"… ma debbono controllare proprio la mia impresa … tra tante?"*, ecc.), tenuta sempre presente la regola del *"neminem laedere"*, del non arrecare danno ad altri.

Nell'impresa, insegnano i giuristi, il principio da osservare è quello della gestione consapevole, informata (quindi fondata sulla conoscenza), e gli economisti sostengono, *"da sempre"*, che la gestione di impresa (sia in un'ottica squisitamente economica, sia nella più ampia ottica sociale) deve essere realizzata sul fondamento di piani, flessibili e scorrevoli, con la consapevolezza che la condizione di governo è connotata da incertezza, e che la delega ad altri senza vigilanza è un modo inaccettabile di gestire perché (come si impara dai processi giudiziari) l'imprenditore, diligente, accorto, *"non può non sapere"* della sua impresa e del mondo socio-economico-giuridico nel quale, l'impresa, sistema aperto ultra complesso, si trova immersa.

Evoluzione tecnologica. Impresa e *privacy*. Armonizzazione e potenziamento. Dalla *privacy* alla *Data Protection*

Negli ultimi anni la tecnologia dell'informazione e della comunicazione nel mondo digitale nel qua-

le viviamo sempre più partecipi delle realtà altrui, cercando di distinguere l'informazione corretta da quella falsa, ci rendiamo conto che le *"vecchie regole"* della *"privacy"*, come nel passato intesa, non possono essere più limitate solo a determinate informazioni *"sensibili"*[1] della persona fisica che lavora/vive nell'impresa, ma debbono essere considerate in un modo più ampio, *"globale"* (il sistema delle informazioni) e, quindi, anche in relazione al mercato, meglio, ai mercati.

Abbiamo fatto un passo avanti. Il nuovo obiettivo è quello dell'adeguata e regolata *Data Protection*.

L'attenzione deve essere ora rivolta non solo al *"Codice della Privacy"*[2] e alle relative disposizioni sanzionatorie[3] o alla disciplina del Codice penale nazionale vigente, o a quella della Legge 18/03/2008, n. 48[4], modificativa del Codice Penale, del Codice di Procedura Penale, del dettato del D.Lgs. 8/06/2001, n. 231 e dello stesso Codice della *privacy*, ma anche al Regolamento (UE) n. 679, del 27 aprile 2016 del Parlamento europeo e del Consiglio.

Il Regolamento in questione, che *"provides a modernised, accountability-based compliance framework for data protection in Europe"*, è applicabile a partire dal 25 maggio 2018 ed è connotato da un significativo sistema sanzionatorio (la parola *"sanzioni"* ricorre ben 48 volte nel testo del provvedimento ove viene specificato che le sanzioni, penali o amministrative, debbono essere *"effettive, proporzionate e dissuasive"*. Ciò secondo quanto rappresentato nel *"considerando"* n. 152[5] e poi statuito[6] per le imprese.

La sanzione è fissata fino al 2% del fatturato mondiale totale annuo dell'esercizio precedente (se superiore), per taluni tipi di violazione, e fino al 4% del fatturato mondiale totale annuo dell'esercizio precedente (se superiore) per altri. Negli altri casi[7], la sanzione è pari, per le violazioni per le quali, per le imprese sono comminate le distinte sanzioni di cui si è detto, rispettivamente, sino ad Euro 10.000.000 e ad Euro 20.000.000.

La materia oggetto della disciplina del Regolamento n. 679/2016 deve essere, poi, posta in relazione con la Direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio del 27 aprile 2016 concernente la *"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 dat*i" ed il cui recepimento deve concretarsi[8] entro il 6 maggio 2018.

Una filosofia globale della *Data Protection*

Il *"considerando n. 13"* rappresenta la *"filosofia globale"* informatrice delle statuizioni del Regolamento:

> *"è necessario un regolamento che garantisca certezza del diritto e trasparenza agli operatori economici, comprese le micro, piccole e medie imprese, offra alle persone fisiche in tutti gli Stati membri il medesimo livello di diritti azionabili e di obblighi e responsabilità dei titolari del trattamento e dei responsabili del trattamento e assicuri un monitoraggio coerente del trattamento dei dati personali, sanzioni equivalenti in tutti gli Stati membri e una cooperazione efficace tra le autorità di controllo dei diversi Stati membri. [..]. Per tener conto della specifica situazione delle micro, piccole e medie imprese, il […] regolamento prevede* (all'art. 30, 5° co.), *una deroga per le organizzazioni che hanno meno di 250 dipendenti* (solo) *per quanto riguarda la conservazione delle registrazioni"*.

Un sistema organizzato, controllato e responsabile

Con il Regolamento siamo in presenza di un sistema impresa che, per la protezione dei dati delle persone fisiche e della loro dinamica in entrata e in uscita, deve porre, indubbiamente, in essere un rafforzamento/modifica per l'adattamento del proprio assetto organizzativo alle nuove regole, un assetto sottoposto, allo scopo, a controllo costante, metodico. Il sistema impresa deve, ragionevolmente, modificare la sua mappatura dei rischi e questo con il ricorso ad esperti interni od esterni dedicati al compito specifico e, pertanto, in possesso di adeguate conoscenze tecniche.

La disciplina del Regolamento prevede non solo un Responsabile titolare del trattamento dei dati[9], ma anche un'attività di tale responsabile[10] volta alla *"protezione dei dati fin dalla progettazione e*

[1] Immagine, reputazione, salute, religione, razza, ecc..
[2] Decreto Legislativo 30 giugno 2003, n. 196 e succ. modd..
[3] Amministrative, *ex* artt. 161-166, penali, *ex* artt. 167-172.
[4] Ratifica ed esecuzione della Convenzione del Consiglio d'Europa sulla criminalità informatica, Convenzione di Budapest del 23 novembre 2001.
[5] Ed agli artt. 83 e 84.
[6] Art. 83, 4° e 5° co..
[7] Persone fisiche non imprese secondo la previsione del *"considerando"* n. 151.
[8] *Ex* art. 63 della Direttiva.
[9] Nel caso di una contitolarità del trattamento, una corresponsabilità.
[10] Art. 25.

protezione per impostazione predefinita"[11].

Nella sostanza il Regolamento *"pone con forza l'accento sulla "responsabilizzazione"* (*accountability* nell'accezione inglese) *di titolari e responsabili - ossia, sull'adozione di comportamenti proattivi e tali da dimostrare la concreta adozione di misure finalizzate ad assicurare la sua applicazione"*[12].

Sono previsti *"codici di condotta"*[13] e sistemi di *monitoraggio*[14] e di *certificazione* volontaria[15] con il ricorso a specifici *organismi accreditati*[16].

Nel contesto, è da ricordare il ruolo dei Revisori interni e del Collegio Sindacale, ruoli, per altro, non modificati, dal Regolamento n. 679/2016, nei principi, ma indubbiamente nelle procedure di controllo e questo per tenere conto dei fattori di rischio propri dell'assetto organizzativo e delle possibili violazioni commesse dalla società o dall'ente imprenditoriale in cui o di cui sono *"verificatori gestionali e contabili"*, a seconda della disciplina di legge che qualifica i soggetti che trattano i dati personali da tutelare.

Non possono essere, poi, ignorati il ruolo e gli specifici compiti dell'Organo di Vigilanza *ex* D.Lgs. n. 231/2001 e successive modifiche alla luce della naturale integrazione tra il Modello organizzativo di cui al predetto Decreto ed i sistemi di gestione aziendale e la gestione include il trattamento e la tutela dei dati, tenuto conto delle tecnologie informatiche e della comunicazione (interna ed esterna) dell'impresa.

Le micro, piccole e medie imprese

Il Regolamento[17], a parte il trattamento particolare, di cui si è detto in relazione al tema delle registrazioni per le imprese con un numero di addetti inferiore ai 250, precisa che *"le istituzioni e gli organi dell'Unione e gli Stati membri e le loro autorità di controllo sono invitati a considerare le esigenze specifiche delle micro, piccole e medie imprese nell'applicare il presente regolamento. La nozione di micro, piccola e media impresa dovrebbe ispirarsi all'articolo 2 dell'allegato della raccomandazione 2003/361/CE*, del 6 maggio 2003 (C(2003) 1422) *della Commissione"* e rinvia alla Commissione ogni opportuna valutazione al fine di *"contemplare misure specifiche per le micro, piccole e medie imprese"*[18].

La disciplina del Regolamento prevede che si prendano (si debbano prendere) in considerazione le specifiche esigenze per le micro e le piccole e medie imprese[19] in relazione ai *"Codici di Condotta"*[20] ed alla *"Certificazione"* volontaria[21].

La Guida dell'*Autorità Garante della Privacy* non rappresenta, tuttavia, un manuale operativo, manuale che deve essere, invece, messo a punto da ogni impresa.

Conclusioni

Con il Regolamento 2016/379 ci si prefigge un obiettivo *"potenziato"* rispetto a quello della tutela della *privacy*. La nuova modalità (e responsabilità) di tutela assume una portata più ampia, coinvolge l'intera architettura del sistema informativo e informatico d'impresa e non può avere confini circoscritti alla sola *privacy*.

Con il Regolamento si formulano norme (giuridico-tecniche) di rafforzamento delle politiche per un più deciso contrasto ai *cybercrime*.

L'integrazione normativa, anche grazie alla Direttiva 2016/680, si realizza, sia a livello nazionale, sia internazionale, sia in termini di *stock*, sia di *flow* dei dati (anche transnazionali e con Paesi *extra* UE). Si pone in essere una concezione di integrazione sistemica (almeno nel contesto dei Paesi dell'UE) con molte altre regole tra le quali quelle della Direttiva 2013/40/EU, del 12 agosto 2013, *"relativa agli attacchi contro i sistemi di informazione"*[22].

Oltre all'UE si debbono considerare anche gli indirizzi dell'OCSE[23] e dell'ONU[24].

Non è, poi, da trascurare la necessaria riconsiderazione delle coperture dei rischi con una ineludibile verifica del *"livello"* della loro assicurazione, anche in relazione all'infedeltà dipendenti

[11] Si vedano, in particolare, tra le altre, *"Data Protection Impact Assessment", "Guidelines on Consent", "Guidelines on Transparency"* -, le *"Guidelines on Data Protection Officers ('DPOs') Adopted on 13 December 2016, revised and adopted on 5 April 2017"*.

[12] In questi termini la Guida del Garante della *privacy* relativa al Regolamento dell'UE.

[13] Art. 40.

[14] Art. 41.

[15] Art. 42.

[16] Art. 43.

[17] *"Considerando"* n. 13.

[18] *"Considerando"* n. 167.

[19] Art. 40, 1° co..

[20] Art. 41.

[21] Art. 42.

[22] Si veda anche la *"Relazione della Commissione al Parlamento Europeo e al Consiglio che valuta in che misura gli Stati membri hanno adottato le misure necessarie per conformarsi alla Direttiva 2013/40/UE relativa agli attacchi contro i sistemi di informazione"*, 13.9.2017, COM(2017) 474 *final*.

[23] *The OECD Privacy Framework*, 2103.

[24] UNITED NATIONS CONFERENCE ON TRADE AND DEVELOPMENT, UNCTAD, *Data protection regulations and international data flows: implications for trade and development*, 2016.

ed ai sistemi (ancorché con l'utilizzo di tecniche di crittografia) di *team viewer* (*extra* aziendale) tipici dei sistemi di teleassistenza informatica e non solo.

Molto lavoro da fare (inclusa la revisione di molti testi contrattuali) ed in tempi contenuti.