CENNI INTRODUTTIVI

Il presente elaborato ha lo scopo di analizzare i contenuti e le novità sostanziali del Regolamento (UE) 2016/679 in materia di *data protection* per verificarne l'impatto sulle Pubbliche Amministrazioni, con precipuo riferimento alle Università statali.

Particolare importanza rivestirà, in questo lavoro, il contributo della Scuola Normale Superiore, nell'ambito del cui Ufficio Affari Legali e Istituzionali lo scrivente ha avuto occasione di sostenere uno stage formativo.

Parimenti rilevanti saranno gli orientamenti delle Autorità garanti in materia di protezione dei dati personali, in relazione sia a quella italiana, sia alle linee guida elaborate dall'*Article 29 Data Protection Working Party* e alle recenti revisioni da parte di gruppi di lavoro di diversi Atenei italiani.

Non sarà trascurato il contesto normativo italiano in materia di amministrazione digitale, che in diverse circostanze deve fare i conti con il contemperamento degli opposti interessi tutelati dal Regolamento sulla protezione dei dati personali, interessi da bilanciare tenendo in considerazione i principi confliggenti e, di volta in volta, parametrandoli al caso concreto. Il riferimento va soprattutto al d.lgs. 33/2013 in materia di trasparenza della Pubblica Amministrazione, novellato dal d.lgs. 97/2016, che ha introdotto anche in Italia il *Freedom Of Information Act* (FOIA)[1] di cui si tratterà più nel dettaglio nel prosieguo, portatore di interessanti aspetti innovativi, ma anche problematici in relazione alla possibile "convivenza sinergica" fra la normativa sulla *data protection*, il diritto di accesso civico generalizzato ai dati della P.A. introdotto dal suddetto decreto e il diritto di accesso documentale agli atti della P.A. stabilito dalla legge n. 241/1990. Ma

[1] Legge introdotta per la prima volta negli Stati Uniti nel 1966, 5 U.S.C. § 552. Ha subito nel corso degli anni diverse modifiche, di cui l'ultima rilevante nel 2007 con l'*Open Government Act*.

non sono da trascurare neppure le recenti innovazioni apportate al CAD[2] dal d.lgs. 179/2016 in materia di riorganizzazione delle Amministrazioni Pubbliche, soprattutto sulla scia dell'emanazione del Regolamento (UE) 2014/910[3], che introducono novità sostanziali nell'operato dei soggetti pubblici in materia di servizi fiduciari. Si tenterà di fornire adottabili soluzioni di carattere tecnico-giuridico sulle priorità e scadenze da osservare per adeguarsi al Regolamento[4], in un'ottica di *compliance* rispetto alle ormai vicinissime innovazioni da applicare per qualunque Pubblica Amministrazione, Università statali comprese.

Infine, si descriverà il sistema di gestione informatica attraverso cui la Scuola Normale Superiore di Pisa protocolla i documenti in entrata e in uscita, denominato "Titulus". Attraverso tale software la Scuola gestisce una mole più che considerevole di documenti, snellendo i tempi di archiviazione, consentendo la velocizzazione dei procedimenti amministrativi e adempiendo al contempo ai propri obblighi di "dematerializzazione" delle procedure. Anche sotto il profilo della sicurezza delle informazioni e della protezione dei dati personali, si cercheranno di dare basilari soluzioni applicative e potenziali suggerimenti per adeguarsi preventivamente al futuro regime di *accountability* che permeerà ogni Pubblica Amministrazione e da cui non sarà possibile astenersi.

[2] Codice dell'Amministrazione Digitale, d.lgs. 7 marzo 2015, n. 82 e successive modifiche e integrazioni.
[3] Il c.d. Regolamento eIDAS sull'identità digitale, che ha introdotto nell'Unione europea una base normativa per i servizi fiduciari e mezzi di identificazione elettronica per gli Stati membri.
[4] Da qui in avanti, anche chiamato GDPR (*General Data Protection Regulation*).

CAPITOLO 1 – IL REGOLAMENTO (UE) 2016/679 IN MATERIA DI *DATA PROTECTION*. LA LENTE DELLE INNOVAZIONI SULLE UNIVERSITÀ ITALIANE

1.1. Il nuovo Regolamento europeo. Breve introduzione

Il GDPR è un Regolamento che prende le mosse da lontano e cerca di inserirsi in una dimensione in perpetua evoluzione[5]. I cambiamenti dell'*information society* sono talmente repentini che risulta realisticamente difficoltoso poterli imbrigliare in un unico provvedimento di carattere normativo, peraltro dal valore vincolante per tutto il territorio eurounitario, con il quale l'intenzione del legislatore europeo è più che ambiziosa e vuole portare a una vera e propria proceduralizzazione nell'utilizzo delle informazioni.

Il quadro normativo su cui si inserisce detto Regolamento è abbastanza variegato, considerando i molteplici provvedimenti comunitari e nazionali che si sono susseguiti negli anni. La c.d. "direttiva madre", ossia la direttiva 95/46/CE, nonostante gli emendamenti e le novità successivi, è per anni rimasta il baluardo della tutela dei diritti e delle libertà fondamentali tra persone fisiche rispetto al trattamento dei loro dati personali e i principi fondamentali sui quali essa è fondata risultano ancora validi; tuttavia, la frammentazione e gli squilibri negli Stati membri nell'implementazione di tutele e garanzie idonee alla *data protection* hanno reso impellente, fra le altre necessità, l'emanazione di un Regolamento che garantisse uno standard minimo di protezione fra gli Stati membri[6].

L'esigenza primaria per l'emanazione del GDPR, comunque, non risiede sull'implementazione di protezioni paritarie. Negli ultimi anni Internet è

[5] Cfr. M. G. STANZIONE, *Il Regolamento europeo sulla privacy: origini e ambito di applicazione*, in *Europa e diritto privato*, 4, 2016, 1249 ss., che nella sua introduzione condensa la travagliata recente storia della protezione dei dati personali.
[6] In questo senso depongono i "considerando" nn. 3, 9 e 10 del GDPR.

divenuto, grazie soprattutto al c.d. *semantic web*[7], all'IoT[8], alle tecnologie *cloud*, ma anche ad altri importantissimi fattori, il principale mezzo per lo *sharing* di informazioni di qualunque carattere. I più importanti *internet service providers* e i *big players* della rete hanno capitalizzato tale condivisione rendendo i dati un'enorme fonte di ricchezza attraverso la raccolta di questi ultimi in forma aggregata[9]. È apparso sempre più chiaro al legislatore europeo che la direttiva 95/46/CE ha mantenuto un aspetto troppo statico, con una conformazione non più adatta all'evoluzione tecnologica degli ultimi anni.

Ragionamento analogo deve farsi per il legislatore nazionale, intervenuto con il d.lgs. 196/2003 per attuare la direttiva 2002/58/CE in materia di protezione dei dati personali e rimpiazzare la vecchia l. n. 675/1996, ma che, nonostante i numerosissimi interventi successivi[10] e una normativa sulla privacy all'avanguardia fra gli Stati europei, ha ancora un corpo normativo che non ha tenuto conto della progressiva realizzazione e implementazione di un mercato digitale europeo.

Il Regolamento 2016/679, peraltro, ha la precisa funzione di inserirsi in un contesto nel quale il dato (*rectius*, l'informazione) diventa appunto il bene giuridico oggetto di un mercato digitale unico[11]. Il legislatore europeo ha ritenuto di dover rimuovere taluni fra i più importanti ostacoli al suddetto mercato, emanando anche il c.d. Regolamento eIDAS[12], con il quale disciplina l'identità online, le firme elettroniche e i servizi fiduciari in generale.

---

[7] Con questa espressione si intende la trasformazione del World Wide Web in un ambiente in cui i documenti pubblicati (pagine HTML, file di qualunque genere ecc.) sono associati a informazioni e dati (i c.d. *metadati*) che ne specificano il contesto semantico in un formato adatto all'interrogazione e all'interpretazione (e.g., il motore di ricerca) e, più in generale, all'elaborazione automatica.

[8] *Internet of Things*, espressione indicante l'estensione del mondo di Internet agli oggetti materiali.

[9] Il c.d. fenomeno dei *big data*.

[10] Sia legislativi, sia di indirizzo, grazie all'operato dell'Autorità Garante italiana.

[11] V., fra gli altri, il *considerando* n. 2 del GDPR.

[12] Regolamento (UE) 2014/910, divenuto applicativo nel luglio 2016.

Nell'ambito delle Pubbliche Amministrazioni, preme evidenziare la necessità di una coerenza da realizzare con altri corpi normativi del nostro ordinamento[13], proprio in relazione al tipo di attività svolta da questi soggetti, alle tipologie di dati trattati e alla trasparenza da garantire nell'ambito, soprattutto, dell'amministrazione digitale.

Il GDPR troverà piena attuazione a partire dal 25 maggio 2018, data a decorrere dalla quale verrà contestualmente e definitivamente abrogata la direttiva 95/46/CE, ma alcune sue parti hanno già trovato immediata applicazione, pertanto fino alla suddetta data il panorama legislativo italiano ospiterà diversi corpi normativi organici.

Sebbene il Regolamento, ad una prima lettura, sembri rispecchiare l'impostazione tradizionale della direttiva madre, cambia profondamente la prospettiva in cui collocare la *data protection*. Anzitutto, il diritto alla protezione dei dati personali assurge ormai a diritto fondamentale, al pari di altri importanti diritti costituzionali quali il diritto alla riservatezza[14]. Inoltre, si è passati ad un approccio non più di tipo meramente formale, bensì di tipo regolatorio fortemente sostanziale, incentrato sulla responsabilità – non più di secondaria importanza – di assicurare e mantenere la conformità al Regolamento su tutti gli Stati membri per tutelare i diritti e le libertà degli interessati.

In linee generali, il GDPR:

[13] In particolare, il d.lgs. 33/2013 e successive modifiche e integrazioni, oltre al C.A.D. (d.lgs. 82/2005 e successive modifiche e integrazioni).

[14] È importante tenere distinti il diritto alla protezione dei dati personali e il diritto alla riservatezza. Il secondo, infatti, nasce molto prima, con la diffusione del mezzo di stampa (un caso famosissimo riconducibile a questo diritto è il caso *Soraya*, cfr. Cass. Civ. 27 maggio 1975, n. 2129) ed è configurabile come una libertà negativa. Il diritto alla protezione dei dati personali è, invece, una libertà *positiva*, perché si permette all'interessato di controllare l'uso dei suoi dati. Questi diritti sono anche disciplinati da due diversi articoli della Carta di Nizza, ovvero all'art. 7 il diritto alla riservatezza e all'art. 8 il diritto alla protezione dei dati personali.

a. Fa conseguire al trattamento e alla protezione dei dati personali una dimensione di autonoma rilevanza all'interno dei processi organizzativi e gestionali di un Ente o di un'azienda;
b. Riafferma tutti i diritti garantiti all'interessato nell'impianto normativo precedente (accesso, rettifica, cancellazione, limitazione, revoca del consenso e opposizione) e ne introduce di nuovi (*data portability*, diritto all'oblio, diritto all'opposizione alla profilazione);
c. Introduce il principio di *accountability*, traducibile più correttamente in "responsabilità e rendicontazione della stessa"[15], che consiste nel porre il titolare e il responsabile del trattamento in una posizione di controllo continuo sulla riduzione del rischio di operazioni non conformi, stimolandoli a comportamenti e prassi virtuose;
d. Fa convergere centralmente il controllo e la *governance* sul rispetto del Regolamento, accrescendo la cooperazione tra Autorità di Controllo nazionali e facendole cooperare con il Comitato, incoraggiando meccanismi di certificazione e rafforzando il sistema sanzionatorio.

1.2. Sintesi delle principali novità del GDPR ed esempi in campo universitario. Nuovo ambito di territorialità e *accountability*

La prima novità da osservare è quella del nuovo ambito di territorialità, che supera il criterio dello stabilimento ed estende l'applicabilità del Regolamento anche ai titolari o responsabili non stabiliti nel territorio dell'Unione, purché il trattamento riguardi l'offerta di beni, servizi o il monitoraggio del comportamento dell'interessato abbia luogo entro i confini

[15] Il concetto di *accountability* è già presente dal 1980 nelle Linee guida della OECD, (Organisation for Economic Cooperation and Development), ma è più volte ripreso dalla dottrina. Cfr., in particolare, G. FINOCCHIARO, *Introduzione al Regolamento europeo sulla Protezione dei Dati*, in *Nuove Leggi Civ. Comm.*, 2017, 1, 1.

UE[16]. Un esempio nell'ambito universitario può certamente essere quello del trattamento che un Ateneo non europeo svolga sui dati personali di uno studente extracomunitario temporaneamente domiciliato nel territorio dell'Unione per il perfezionamento dei suoi studi[17]. In tal senso, pertanto, non è necessario essere cittadini comunitari per beneficiare delle tutele dal Regolamento, ma è sufficiente essere collocati nel "territorio operativo" del GDPR.

All'art. 24 si definisce la responsabilità del titolare del trattamento, che dev'essere in grado di mettere in atto "*misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al presente regolamento*". Nella specie, dovrà essere in grado di dimostrare la conformità del trattamento tenendo conto della natura, dell'obbligo, del contesto e delle finalità del trattamento, oltre ai rischi sulle libertà e i diritti delle persone fisiche[18].

1.2.1. *Privacy by design*, *privacy by default* e pseudonimizzazione

Sull'articolo 25[19] del Regolamento (UE) 2016/679 è posto un accento particolare con riferimento all'introduzione di misure preventive di sicurezza a tutela dell'interessato nel trattamento dei suoi dati. Ciò costituisce concreta traduzione del summenzionato principio di *accountability*.

---

[16] In tal senso depongono i *considerando* da 14 a 27 e l'art. 3 del Regolamento. Tuttavia, il *considerando* 26 fa salvi i trattamenti effettuati su informazioni anonime, ovvero quelle informazioni non riferibili a persona fisica identificata o identificabile o a dati personali resi sufficientemente anonimi da impedire o da non consentire più l'identificazione dell'interessato.

[17] L'esempio, come molto altro materiale nel prosieguo, è tratto dagli studi del Gruppo di lavoro "Linee guida Privacy e GDPR" del Convegno dei Direttori Generali delle Amministrazioni Universitarie, che sta lavorando sull'adozione di soluzioni concrete per la corretta applicabilità del Regolamento negli Atenei nazionali.

[18] Ciò è previsto all'art. 25, paragrafo 1 del Regolamento.

[19] Ma, prima ancora, dal *considerando* n. 78, il quale afferma che "*la tutela dei diritti e delle libertà delle persone fisiche relativamente al trattamento dei dati personali richiede l'adozione di misure tecniche e organizzative adeguate per garantire il rispetto delle disposizioni del presente regolamento* […]".

Nella specie, al paragrafo 1 si prevede – attraverso il concetto di *privacy by design* – che il titolare del trattamento debba prevedere fin dalla progettazione dello strumento buone prassi di protezione dei dati personali mediante l'applicazione del principio di *minimization* relativo ai dati personali oggetto di trattamento, sia con riguardo alla quantità di dati da trattare, che con riguardo alla c.d. *data retention*[20] e alla pseudonimizzazione[21], ovvero l'oscuramento reversibile dei dati identificativi del soggetto interessato. *Case-by-case*, pertanto, occorrerà stabilire le concrete misure da adottare in relazione al tipo di dato trattato.

Nell'ambito universitario, un esempio di *minimization* che il titolare (l'Università statale) dovrebbe porre in essere relativamente ad un concorso per l'accesso a corsi di studi è certamente la richiesta solo dei dati atti a verificare lo *status* di "non studente" del (o della) partecipante. Tutti i dati necessari ad un'eventuale fase successiva (quella relativa alla possibile immatricolazione) dovranno essere oggetto di un trattamento successivo e differente rispetto al primo. Per quanto invece riguarda un esempio concreto di pseudonimizzazione in campo accademico, la comunicazione mediante la quale l'Università stabilisce quali studenti dovranno recarsi in una determinata aula per sostenere una procedura concorsuale (soprattutto se effettuata via Internet) dovrebbe essere pseudonimizzata indicando solo un ID numerico[22], o addirittura anonimizzata prevedendo un'aggregazione alfabetica per associare l'aula al candidato; quest'ultima tecnica, tuttavia, costituisce una diversa soluzione, che verrà analizzata *infra*.

Nel secondo paragrafo dell'articolo 25 – qui, invece, si tratta di *privacy by default* – è previsto che il titolare del trattamento debba mettere in atto

[20] Il periodo di tempo di conservazione del dato.

[21] Sul tema cfr. L. BOLOGNINI-C. BISTOLFI, *Pseudonymization and impacts of Big (personal/anonymous) Data processing in the transition from the Directive 95/46/EC to the new EU General Data Protection Regulation*, in *Computer Law & Security Review*, 33, 2017, 179 ss.

[22] Nella bozza di linee-guida revisionate dal Gruppo di lavoro del CODAU viene suggerito un "pre-matricola".

misure tecniche e organizzative adeguate per garantire che siano trattati solo i dati necessari per ogni specifica finalità del trattamento (secondo il già collaudato principio di non eccedenza). Nel contesto che ci riguarda, pertanto, sarà necessario ad esempio curare capillarmente le diverse autorizzazioni di lettura e di modifica dei dati all'interno dei database in base al profilo del soggetto legittimato al trattamento (*e.g.*, attraverso un sistema di *mandatory access control*[23]).

1.2.2. Il DPIA, l'obbligo di notifica di violazione dei dati personali all'Autorità di Controllo e il Registro dei trattamenti. Le "nuove" sanzioni

Il DPIA (*Data Protection Impact Assessment*), o valutazione d'impatto, è trattato dal Regolamento nei *considerando* da 89 a 96, nonché negli articoli 35 e 36. Si tratta di un'attività effettuata su aree specifiche per identificare e minimizzare i rischi di non conformità al Regolamento, che viene richiesta per trattamenti su larga scala, effettuati mediante nuovi mezzi tecnologici ad elevato rischio che comportino l'implementazione di trattamenti di profilazione[24], sorveglianza, utilizzo di dati particolari (biometrici, giudiziari, sensibili)[25]. In un periodo storico in cui la pervasività di Internet coinvolge

[23] Un sistema di sicurezza dei dati mediante il quale vengono creati diversi livelli di informazioni. Coloro che controllano questi sistemi fissano per ciascun utente non solo il livello massimo di informazioni a cui può accedere, ma anche il livello minimo nel quale si possono scrivere e modificare documenti. Non è possibile, ad esempio, scrivere in livelli di *confidenciality* più bassa.

[24] Il GDPR la definisce, all'art. 4, n. 4, come "*qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti 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*".

[25] Sulla DPIA e per capire meglio lo strumento in chiave applicativa v. in particolare ARTICLE 29 DATA PROTECTION WORKING PARTY, *Linee-guida concernenti la valutazione di impatto sulla protezione dei dati nonché i criteri per stabilire se un trattamento "possa presentare un rischio elevato" ai sensi del regolamento 2016/679*, scaricabili nella traduzione italiana su http://194.242.234.211/documents/10160/0/WP+248+-+Linee-guida+concernenti+valutazione+impatto+sulla+protezione+dati. Lo studio del gruppo di lavoro offre interessanti spunti, anche nei suoi due allegati, con particolare riferimento ad

sempre più spesso i dati personali, l'importanza delle valutazioni sugli eventuali rischi e responsabilità conseguenti assume un carattere fondamentale, posto che il precedente approccio formalistico basato sul binomio informativa-consenso è risultato spesso fallace[26] per i suddetti fini.

La redazione dell'elenco delle tipologie di trattamenti soggetti a DPIA è rimessa all'Autorità di Controllo, che lo comunica al Comitato europeo per la protezione dei dati[27]. La valutazione d'impatto, secondo il classico modello dell'analisi del rischio, dovrà contenere almeno:

a. una descrizione sistematica dei trattamenti previsti, delle finalità e dell'eventuale ricorrenza di un legittimo interesse perseguito dal titolare del trattamento;
b. una valutazione sulla necessità e la proporzionalità dei trattamenti in relazione alle finalità;
c. una valutazione dei rischi per i diritti e le libertà degli interessati;
d. le misure organizzative e tecniche previste per garantire la protezione dei dati personali e la conformità al Regolamento[28].

Per le Università statali detto approccio alla gestione del rischio è di particolare evidenza, considerando la sovente eventualità di effettuare trattamenti su larga scala su base tecnologica. L'Università, supportata dal proprio *data protection officer*[29], dovrà valutare preventivamente l'impatto dei propri trattamenti sui dati personali dei vari interessati in sinergia con l'operato e gli orientamenti dell'Autorità di Controllo. L'Ateneo, infatti,

esemplificazioni di DPIA in altri Stati europei. È molto forte la correlazione posta dal Working Party fra il DPO e la DPIA, che sinergicamente garantiscono il rispetto, da parte del titolare, del principio di *accountability*.

[26] A. MANTELERO, *Responsabilità e rischio nel Regolamento UE 2016/679*, in *Le nuove leggi civili commentate*, 2017, 1, 156 ss. In particolare, viene sostenuto dall'A. che lo strutturare il diritto alla protezione dei dati personali come diritto individuale, nonostante le corti lo interpretino nella sua dimensione sociale, mostra i suoi limiti nell'attuale contesto degli algoritmi predittivi e di dati trattati in forma aggregata.

[27] Previsto agli artt. 68 ss. del GDPR.

[28] Art. 35, paragrafo 7 del GDPR.

[29] Di cui si tratterà meglio *infra*.

consultandosi con il Responsabile per la protezione dei dati personali, dovrebbe preventivamente stabilire delle linee-guida afferenti alle DPIA sui casi, le metodologie e le salvaguardie da applicare. L'esempio più immediato è quello delle riprese effettuate dagli impianti di videosorveglianza con particolari tecnologie (capaci, ad esempio, di rilevare dati biometrici[30] sulla base del riconoscimento facciale). Quello della DPIA è un argomento particolarmente complesso e frastagliato, coinvolgente moltissime altre questioni, che non è possibile approfondire dettagliatamente in questa sede.

I *considerando* nn. 83 e 84, nonché la Sezione II del Capo IV del Regolamento, si occupano sia delle idonee misure di sicurezza che il titolare dovrebbe adottare per la riduzione dei rischi, sia della notifica all'Autorità di Controllo in caso di violazione dei dati personali (c.d. *data breach*).

Fra le misure previste, il legislatore europeo fa riferimento alla pseudonimizzazione, cifratura, capacità di assicurare riservatezza, integrità, disponibilità e resilienza del dato, la capacità di tempestivo ripristino dei dati stessi in caso di incidente fisico o tecnico, oltre che una procedura di *audit* per verificare regolarmente l'efficacia delle suddette misure[31]. L'articolo 32, paragrafo 4, impedisce a chiunque agisca sotto la loro autorità (e non sia stato istruito in tal senso dal titolare o dal responsabile) di trattare i dati personali.

Nell'eventualità di un *data breach*, il Regolamento predispone delle misure innovative rispetto alla prassi normativa antecedente, anzitutto formulando una definizione compiuta di violazione dei dati personali all'articolo 4, paragrafo 1, n. 12[32], nonché prevedendo – e ciò costituisce la novità più importante in merito – l'obbligo per il titolare di comunicare all'Autorità di Controllo l'avvenuta violazione dei dati personali entro e non

[30] Per la definizione di dato biometrico si rimanda all'art. 4, n. 14 del GDPR.
[31] Articolo 32, paragrafo 1 del GDPR.
[32] Viene definita come "*la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati*".

oltre 72 ore dall'acquisizione della conoscenza dell'accadimento, con la descrizione di:

- natura, categorie, numero approssimativo degli interessati e numero approssimativo di registrazioni dei dati in questione;
- dati di contatto del DPO;
- probabili conseguenze del *data breach*;
- le misure che si intendono adottare per ridurre o scongiurare gli effetti negativi della violazione.

Ai sensi dell'articolo 34, la comunicazione della violazione dei dati personali all'interessato va compiuta quando il *data breach* comporta elevati rischi per i diritti e le libertà dello stesso.

Una simile evenienza potrebbe verificarsi nelle Università statali qualora fosse violato il sistema informativo di gestione dei dati di login per studenti e personale tale da creare un concreto pericolo per le credenziali gestite dal sistema. In tal caso il titolare valuta, sulla base della tipologia e dell'entità della violazione, se notificarla all'Autorità di Controllo e/o comunicarla agli interessati coinvolti[33].

Un ulteriore sforzo del legislatore europeo per rendicontare l'attività svolta dal titolare e/o dal responsabile di trattamento è certamente la previsione dei Registri per le attività di trattamento[34], che devono contenere i riferimenti di contatto di queste figure oltre che quelli del DPO, la descrizione degli interessati e dei destinatari, le categorie dei dati personali trattati, la presenza di trasferimenti di dati verso un Paese terzo o un'Organizzazione internazionale unitamente alla documentazione sulle appropriate garanzie,

[33] Il Gruppo di lavoro delle "Linee Guida Privacy e GDPR" fa riferimento a diversi scenari, sulla base della tipologia di archiviazione del dato ei sistemi informatici degli Atenei. In generale, non è mai consigliabile archiviare "in chiaro" le credenziali dei login, ma è opportuno perlomeno cifrarle mediante *hash* irreversibile e, per maggior scrupolo, utilizzare una gestione separata dei sistemi di login rispetto alle risorse che li identificano.
[34] *Considerando* n. 83 e articolo 30 del GDPR, tematica approfondita *infra*.

la tempistica della cancellazione dei dati, nonché la descrizione delle misure di sicurezza e organizzative adottate.

Gli obblighi derivanti dal Regolamento, come i diritti e le libertà da esso tutelati, divengono oggetto di un apparato sanzionatorio del tutto rinnovato e ben più temibile di quello precedente, soprattutto per le imprese[35]. Per le PP.AA. sono previste sanzioni amministrative pecuniarie fino alla somma di € 20.000.000,00 fatto salvo il diritto al risarcimento del danno, che può incidere enormemente sul buon andamento dell'Amministrazione stessa[36].

1.3. Nuovi diritti: limitazione, opposizione alla profilazione, diritto all'oblio, *data portability*

I nuovi diritti si aggiungono a quelli "riconfermati" e ne estendono o rafforzano l'ambito di applicazione. Sono previsti agli articoli 18, 20, 21 e 22.

Il diritto di limitazione è un'estensione del diritto di blocco previsto dal Codice privacy, tramite il quale è possibile, appunto, limitare il trattamento dei dati anche in assenza di utilizzo illecito di questi da parte del titolare, ove sia in pendenza una richiesta di rettifica o di opposizione al trattamento formulate dall'interessato ai sensi degli artt. 16 e 21 del GDPR.

In condizioni di limitazione e con la sola eccezione della conservazione, ogni altro trattamento potrà essere effettuato solo con il consenso dell'interessato, l'accertamento dei diritti in sede giudiziaria, la tutela dei diritti di altra persona (fisica o giuridica), o la presenza di un interesse pubblico rilevante.

Il diritto di opposizione trova spazio nelle ipotesi di profilazione. Tale diritto è necessariamente connesso a una situazione particolare

[35] Le sanzioni pecuniarie possono arrivare, per le imprese, fino al 4% del fatturato mondiale totale annuo dell'esercizio precedente.

[36] Le sanzioni sono previste all'articolo 83 del GDPR. È bene far presente, comunque, che il paragrafo 7 del medesimo articolo prevede la possibilità, per ogni Stato membro, di far salve le norme nazionali che dispongono se e in che misura possono essere inflitte sanzioni amministrative pecuniarie ad autorità pubbliche e organismi pubblici istituiti in tale Stato membro.

dell'interessato (che può essere legata a vari fattori, fra cui il rendimento professionale, stato di salute, situazione economica, ecc.) e riconosce a quest'ultimo la possibilità di opporsi e bloccare il trattamento, salvo l'onere probatorio in capo al titolare di dimostrare l'esistenza di "motivi legittimi cogenti"[37] che prevalgano sugli interessi, diritti e libertà dell'interessato, oppure l'esercizio o la difesa di un diritto in sede giudiziaria.

Il c.d. "diritto all'oblio" è un – a lungo discusso – diritto alla cancellazione dei propri dati personali in forma rafforzata[38] nel caso in cui questi siano resi pubblici online[39]. I titolari devono informare della richiesta di cancellazione ogni altro titolare che tratta i dati da eliminare, compresi "*qualsiasi link, copia o riproduzione*". L'interessato può, inoltre, sempre chiedere la cancellazione dei propri dati a seguito della revoca del consenso al trattamento.

Il diritto alla *data portability* consiste nell'affermazione del diritto, da parte del *data subject*, di poter richiedere e ricevere in un formato strutturato, di uso comune e leggibile da dispositivo automatico i dati personali che lo riguardano. L'interessato può anche richiedere la trasmissione di tali dati da un titolare ad un altro, senza necessariamente volere la cancellazione di essi sui *database* del primo. Lo scopo del Regolamento è di certo quello di facilitare l'interscambio di informazioni digitali nel territorio eurounitario[40].

---

[37] Art. 21, paragrafo 1 del GDPR.

[38] Il caso spartiacque, che ha dato vita alla grande "diatriba" intorno a questo diritto, è rappresentato dall'ormai più che famoso caso *Google Spain SL – Google Inc. c. Agencia Española de Protección de Datos (AEPD) – Mario Costaja González*, causa C-131/12 deciso dalla Corte di Giustizia dell'Unione europea, con il quale si afferma la priorità della privacy del soggetto rispetto all'interesse economico perseguito dal *service provider*. Per maggiori approfondimenti cfr., *inter multis*, F. MELLIS, *Il diritto all'oblio e i motori di ricerca nel diritto europeo*, in *Giornale Dir. Amm.*, 2015, 2, 171 ss., oppure F. RUSSO, *Diritto all'oblio e motori di ricerca: la prima pronuncia dei Tribunali italiani dopo il caso Google Spain – il commento*, in *Danno e resp.*, 2017, 3, 299 ss. Rimane fermo che il diritto alla cancellazione rafforzata di cui all'articolo 17 del GDPR è un diritto dai connotati differenti rispetto al diritto all'oblio così come interpretato dalla Corte di Giustizia dell'Unione europea.

[39] Sulla materia cfr. F. DI CIOMMO, *Il diritto all'oblio (oblito) nel regolamento Ue 2016/679 sul trattamento dei dati personali*, in *Il Foro it.*, 2017, V, 306 ss.

[40] Cfr. ARTICLE 29 DATA PROTECTION WORKING PARTY, *Guidelines on the right to data portability*, adottate nel dicembre 2016 e revisionate nell'aprile 2017, liberamente consultabili su https://ec.europa.eu/newsroom/document.cfm?doc_id=44099.

Per le Università statali si tratta di un diritto di rilievo residuale, poiché tale diritto viene applicato solo ai dati trattati con il consenso dell'interessato (o sulla base di un contratto stipulato con l'interessato) e solo su quei dati che sono stati "forniti" dal *data subject* al titolare, non essendo previsto per i dati trattati sulla base di un interesse pubblico o connesso all'esercizio di pubblici poteri del titolare[41]. Tuttavia, ad avviso dello scrivente, le Università dovrebbero garantire uniformità di trattamento anche in un'ottica di condivisione informativa tra Atenei, comportando così per gli interessati anche soltanto la semplificazione delle procedure burocratiche in contesti che coinvolgono istituti universitari differenti[42].

1.4. I nuovi (e i vecchi) soggetti del Regolamento

Il GDPR riformula "l'organigramma" dei soggetti che prendono parte al trattamento dei dati personali, aggiungendo nuove, importantissime figure che specialmente per le PP.AA. (e dunque anche per gli Atenei) ricopriranno un ruolo di prim'ordine sulla tutela dei dati personali nel nuovo quadro descritto dal legislatore europeo. Insieme ad essi, peraltro, viene configurato un nuovo sistema per la corretta applicazione del Regolamento, più efficace e deflazionistico – proprio in quanto proattivo e non più reattivo – del contenzioso giudiziario.

Il titolare del trattamento (o *data controller*) è definito come "*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*"[43]. Ne consegue che si assume la qualifica di titolare nel momento in cui si raccolgono dati allo scopo di trattarli per finalità lecite. In ambito universitario il titolare è l'Ateneo nel suo complesso (è appunto

[41] Articolo 20, paragrafo 3 del GDPR.
[42] Ad esempio, per garantire un interscambio informativo rapido nelle ipotesi di progetto Erasmus o di *double degree*.
[43] Articolo 4 del GDPR.

l'Università che determina le finalità e i mezzi del trattamento), il cui rappresentante legale è ravvisabile nella persona del Rettore. Sul profilo delle responsabilità, è corretto prevedere dei meccanismi di *compliance* e *audit* efficaci, in ragione del fatto che la catena di distribuzione degli incarichi spesso disgrega gli strumenti di controllo sulla corretta applicazione del Regolamento e sul trattamento dei dati personali; per tali motivi, la legge e/o lo Statuto dell'Ateneo devono necessariamente prevedere con trasparenza come i compiti in quest'ambito siano suddivisi. Il titolare, infatti, risponde della corretta applicazione della normativa sulla *data protection*.

Il medesimo discorso vale per i contitolari (*joint controllers*) che trattano i dati insieme al titolare e determinano le modalità di trattamento congiuntamente ad esso. I contitolari collaborano al raggiungimento delle finalità del trattamento condivise con il *controller*, divenendo responsabili in solido nei confronti dell'interessato.

Le disposizioni relative al responsabile del trattamento (*data processor*) differiscono rispetto alla disciplina prevista per tale soggetto nel previgente Codice privacy; infatti, nel GDPR il responsabile risponde solidalmente con il titolare (ed eventuali contitolari) delle inadempienze rispetto al trattamento dei dati personali relativi all'interessato. All'interno di una struttura ramificata come quella dell'Università, è utile effettuare una distinzione; possono esistere, infatti, responsabili che il titolare istruisce opportunamente (i quali, molto spesso, sono rappresentati dai dirigenti delle strutture interne o comunque figure di rilievo organizzativo) all'adeguamento dei propri uffici rispetto agli obblighi e alle buone prassi derivanti dal GDPR, i c.d. "responsabili interni"[44]. In ulteriori casi, invece, il responsabile del trattamento può non essere "interno" all'organizzazione, bensì la persona (fisica o giuridica) che gestisce alcune tipologie di dati personali per servizi applicativi in *hosting* o *outsourcing* per conto dell'Ateneo, quindi con

[44] Così vengono definiti dagli studiosi che hanno elaborato le bozze delle linee guida in materia di privacy e protezione dei dati personali in ambito universitario.

un'autonoma attività e anch'esso con una responsabilità in solido rispetto al titolare. Ad esempio, nel caso della Scuola Normale Superiore, il CINECA[45] rappresenta un responsabile per il trattamento con riguardo ai numerosi dati trattati mediante l'applicativo "Titulus". Il responsabile deve garantire all'interessato lo stesso livello di garanzie e tutele offerto dal titolare. È utile, in questo senso, la stipulazione di accordi con apposite clausole contrattuali che indichino gli ambiti di responsabilità. Il Regolamento, in tal senso, ritiene bastevole l'adozione e l'applicazione sia di codici di condotta *ex* art. 40 del GDPR, sia certificazioni approvate ai sensi dell'articolo 42. Fondamentale, in questo sistema, è la necessità da parte del titolare di aver pieno controllo sulla catena delle responsabilità, venendo informato dell'esistenza di ogni eventuale sub-responsabile.

Con riferimento alla figura dei c.d. soggetti autorizzati, nulla differisce rispetto alla disciplina italiana previgente[46], ma in questo caso è da ribadire con forza la necessaria istruzione di tali soggetti da parte del DPO in vece del titolare, intesa come formazione specifica, con percorsi formativi adeguati per garantire il pieno rispetto del Regolamento.

Il destinatario (*recipient*) è definito all'articolo 4 come "*la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che riceve comunicazione di dati personali, che si tratti o meno di terzi*". Possono essere considerati destinatari tutti i soggetti che, sia per l'esecuzione di trattamenti in proprio, sia per il trattamento per conto del titolare, ricevono da parte dello stesso dati personali. È importante per gli Atenei elencare nelle informative ciascun destinatario e/o ciascuna categoria di destinatari per sottoporli all'attenzione dell'interessato.

[45] Consorzio Interuniversitario del Nord-Est per il Calcolo Automatico.

[46] Cfr. AUTORITÀ GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Guida all'applicazione del Regolamento europeo per la protezione dei dati personali*, su http://www.garanteprivacy.it/guida-all-applicazione-del-regolamento-europeo-in-materia-di-protezione-dei-dati-personali.

Il destinatario può essere un soggetto "terzo" o meno. Se, nel ricevere dati personali dal titolare, perseguirà finalità proprie per il trattamento, diventerà un separato titolare in relazione a tali ultime finalità, come il caso del consorzio interuniversitario "AlmaLaurea", che si occupa dell'inserimento dei laureati nel mondo del lavoro. In tal caso, il destinatario deve impegnarsi a fornire all'interessato l'informativa sul trattamento nel minor tempo possibile, a meno che lo stesso non disponga già dell'informazione o tale adempimento richieda uno sforzo sproporzionato. Per le finalità espressamente previste dalla legge con riguardo alla comunicazione di dati ad altri soggetti (come nel caso dell'INPS per il trattamento ai fini pensionistici) non è richiesto l'obbligo di informativa né da parte del titolare, né da parte del destinatario.

L'interessato (*data subject*) è la persona fisica al quale si riferiscono o sono riferibili i dati trattati. I diritti di cui dispone sono già stati definiti *supra*[47]. Nell'ambito universitario statale può rientrare fra le categorie di interessati una vasta gamma di soggetti, che va dal privato cittadino al personale tecnico-amministrativo, compresi assegnisti, collaboratori, studenti, dottorandi, ecc. Per ogni categoria di interessati potranno essere coinvolti dati e interessi diversi, ragion per la quale molto spesso le informative dovranno variare nel loro contenuto e prevedere ipotesi e diritti differenti.

Le Autorità di Controllo, infine, sono incaricate di "*sorvegliare l'applicazione del presente regolamento al fine di tutelare i diritti e le libertà fondamentali delle persone fisiche con riguardo al trattamento e di agevolare la libera circolazione dei dati personali all'interno dell'Unione*"[48]. A livello comunitario, nel caso in cui in un singolo Stato membro siano più d'una, va designata quella che le rappresenterà al Comitato europeo per la protezione dei dati, con funzione di coordinamento fra di esse. Tale Comitato avrà poi funzioni di supporto alla Commissione europea. Alle varie Autorità di

[47] Par. 1.3, 12 ss.
[48] Articolo 51, numero 1 del GDPR.

Controllo nazionali spettano le decisioni sui reclami presentati dagli interessati.

1.4.1. Il *data protection officer* (DPO)

Separate considerazioni merita l'introduzione della nuova figura del Responsabile per la Protezione dei Dati personali (RPD), o *data protection officer* (DPO)[49], che svolge un ruolo di primario rilievo con riferimento alle Pubbliche Amministrazioni, nelle quali la sua nomina è prevista come obbligatoria da parte del Regolamento[50]. Questa figura indipendente, già prevista in Paesi come Germania, Belgio, Francia, Paesi Bassi e Lussemburgo[51], assurge a punto di collegamento fra Autorità di Controllo e titolari del trattamento. L'Università può prevedere la nomina di un DPO esterno o interno, previa verifica della mancanza di un conflitto di interessi; può disporre che, nel caso di trattamenti complessi di dati, a svolgere tale funzione sia un gruppo di persone piuttosto che un singolo, ferma restando l'indicazione di una persona specifica come riferimento per l'Ente. Il DPO deve essere indipendente, sottoposto a vincolo di segretezza sui dati personali oggetto della sua attività, dev'essere dotato di risorse adeguate all'adempimento del suo compito, avere un insieme di conoscenze informatiche e giuridiche[52].

Al Responsabile per la Protezione dei Dati va dato ampio accesso alle informazioni e dev'essere interpellato ogniqualvolta si presentino

---

[49] Sulle origini della figura risulta utile il saggio di V. AMENTA, *Il Regolamento UE 2016/679 e la nascita del* data protection officer, in D. POLETTI-P. PASSAGLIA (cur.), *Nodi virtuali, legami informali: Internet alla ricerca di regole*, 2017, Pisa University Press, 77 ss.

[50] La figura del *data protection officer* è prevista nella sezione 4 del Capo IV del Regolamento (UE) 2016/679.

[51] Cfr. G. FINOCCHIARO, *Introduzione al Regolamento*, op. cit.

[52] Cfr. AGENZIA PER L'ITALIA DIGITALE, in collaborazione con Bird & Bird, *Il Regolamento (UE) 2016/679 e la digitalizzazione delle PA: quale impatto?*, consultabile su http://www.agid.gov.it/sites/default/files/presentazioni/03-il_regolamento_europeo_sulla_protezione_dei_dati_cococloud_5_10_2016.pdf

problematiche relative al trattamento e alla protezione dei dati personali. Vigila sul corretto adempimento degli obblighi derivanti dal Regolamento, attivandosi per proteggere i dati personali degli interessati attraverso i meccanismi di *privacy by design* e *privacy by default*. Ha il compito di coadiuvare il titolare del trattamento dei dati nel DPIA e nella redazione del Registro dei trattamenti, nonché di compiere attività di *auditing* per verificare il rispetto del GDPR nell'Ateneo. Importantissimo compito assegnatogli è quello di fornire consulenze e chiarimenti ai titolari/responsabili del trattamento, oltre che al personale interno preposto al trattamento dei dati personali in applicazione del Regolamento. In ragione dell'importanza di tale figura – che diventa il riferimento per tutti i soggetti legati alla *data protection* – i recapiti relativi al DPO devono essere ampiamente pubblicizzati, nonché presenti nell'informativa per l'interessato[53].

L'*Article 29 Data Protection Working Party* ha elaborato e suggerito dei meccanismi di salvaguardia per garantire al DPO l'indipendenza e la mancanza di conflitti di interessi[54]. Sui compiti più cogenti dei DPO con riguardo alle Università statali, si tornerà *infra*.

1.5. Brevi cenni all'articolo 89 e rinvio

L'articolo 89 del Regolamento (UE) 2016/679 è rubricato "Garanzie e deroghe relative al trattamento a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici" e prevede quanto segue:

> "*1. Il trattamento a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici è soggetto a garanzie adeguate per i diritti e le libertà dell'interessato, in conformità del presente regolamento. Tali garanzie assicurano che siano state predisposte misure tecniche e organizzative, in particolare al fine di garantire il rispetto del principio della*

[53] Per ulteriori chiarimenti, v. le linee guida del Garante sul DPO consultabili su http://www.garanteprivacy.it/rpd.

[54] In tal senso cfr. ARTICLE 29 DATA PROTECTION WORKING PARTY, *Guidelines on Data Protection Officers (DPOs)*, adottate il 13 dicembre 2016 e revisionate il 5 aprile 2017, 24 ss., scaricabili su https://ec.europa.eu/newsroom/document.cfm?doc_id=43823.

minimizzazione dei dati. Tali misure possono includere la pseudonimizzazione, purché le finalità in questione possano essere conseguite in tal modo. Qualora possano essere conseguite attraverso il trattamento ulteriore che non consenta o non consenta più di identificare l'interessato, tali finalità devono essere conseguite in tal modo.

2. Se i dati personali sono trattati a fini di ricerca scientifica o storica o a fini statistici, il diritto dell'Unione o degli Stati membri può prevedere deroghe ai diritti di cui agli articoli 15, 16, 18 e 21, fatte salve le condizioni e le garanzie di cui al paragrafo 1 del presente articolo, nella misura in cui tali diritti rischiano di rendere impossibile o di pregiudicare gravemente il conseguimento delle finalità specifiche e tali deroghe sono necessarie al conseguimento di dette finalità.

3. Se i dati personali sono trattati per finalità di archiviazione nel pubblico interesse, il diritto dell'Unione o degli Stati membri può prevedere deroghe ai diritti di cui agli articoli 15, 16, 18, 19, 20 e 21, fatte salve le condizioni e le garanzie di cui al paragrafo 1 del presente articolo, nella misura in cui tali diritti rischiano di rendere impossibile o di pregiudicare gravemente il conseguimento delle finalità specifiche e tali deroghe sono necessarie al conseguimento di dette finalità.

4. Qualora il trattamento di cui ai paragrafi 2 e 3 funga allo stesso tempo a un altro scopo, le deroghe si applicano solo al trattamento per le finalità di cui ai medesimi paragrafi."

Il primo comma dell'articolo 89 si riferisce al trattamento ai fini di archiviazione nel pubblico interesse, ricerca scientifica, storica o ai fini statistici. Pone in chiaro che la raccolta di dati personali da trattare ai fini predetti deve essere effettuata nel pieno rispetto delle libertà e delle tutele garantite del GDPR, prevedendo l'utilizzo di determinate misure (come la pseudonimizzazione, che il legislatore europeo prevede a titolo esemplificativo) che garantiscano la *minimization* dei dati trattati.

Gli aspetti interessanti, tuttavia, pervengono ai paragrafi successivi, nei quali si consentono delle deroghe favorevoli ai titolari che trattino i dati per i suddetti fini. In particolare, al paragrafo 2 si consente di "limitare" molti dei diritti dell'interessato (nella specie, accesso, rettifica, limitazione e opposizione al trattamento) qualora essi possano rendere impossibile o pregiudicare gravemente il conseguimento delle finalità specifiche e ciò sia necessario al raggiungimento degli scopi di ricerca scientifica o storica, o a

fini statistici; al paragrafo 3, invece, si limitano, oltre ai diritti appena nominati, anche quelli *ex* artt. 19 e 20, ossia il diritto relativo all'obbligo, da parte del titolare, di notifica in caso di rettifica, cancellazione o limitazione dei dati e il diritto alla *data portability* dell'interessato, nel caso di perseguimento delle finalità di archiviazione nel pubblico interesse. Questi due paragrafi "allargano le maglie" alla ricerca per poter permettere ai titolari di trattare lecitamente alcune categorie di dati in relazione alle suddette finalità. A temperare tali limitazioni, comunque, interviene il quarto e ultimo paragrafo, che prevede infatti una scissione fra il trattamento (o la parte del trattamento) ai fini di archiviazione, ricerca scientifica o storica, statistici e il trattamento (o la parte del trattamento) che abbia uno scopo differente. In tal caso, le deroghe ai diritti degli interessati si applicano solo ai primi scopi[55]. Infatti, l'interessato potrà opporsi *ex* art. 21, par. 6, salvo che il trattamento sia effettuato nell'esecuzione di un interesse pubblico.

L'Università gestisce una grande mole di progetti di ricerca, molti dei quali coinvolgenti dati personali di diverse categorie di interessati. Il Regolamento, come già esposto, semplifica le modalità di trattamento di tali dati, consentendo ai titolari di non sentirsi eccessivamente "vincolati" dai limiti normativi imposti dalla protezione dei dati personali. Tuttavia, proprio per la particolare importanza che tale tipologia di trattamento riveste per gli Atenei e per gli interessi coinvolti nella ricerca e nell'uso a fini statistici di queste informazioni, nel prosieguo si specificheranno più nel dettaglio i presupposti, la raccolta e l'elaborazione di tali dati[56].

[55] L'interpretazione che deve essere data all'articolo, comunque, non dovrebbe essere troppo ampia, come chiarito anche dal Garante Privacy europeo (European Data Protection Supervisor) in una presentazione consultabile su http://www.ema.europa.eu/docs/en_GB/document_library/Presentation/2017/01/WC500219338.pdf.

[56] V. *infra*, capitolo III.