Direttore dei servizi generali e amministrativi

Percorso formativo

“Abilitare l'innovazione”

Pordenone, 7 novembre 2017

Formatore: Susanna Granello

Area 2 - Gestione e organizzazione

1. *Organizzazione del lavoro, collaborazione e realizzazione di modelli di lavoro in team;*
2. *amministrazione digitale, sicurezza dei dati e privacy.*

Area 2 – Gestione e organizzazione

Organizzazione del lavoro, collaborazione e realizzazione di modelli di lavoro in *team*; amministrazione digitale, sicurezza dei dati e *privacy* *(6 ore)*.

Area 3 – Le azioni del PNSD

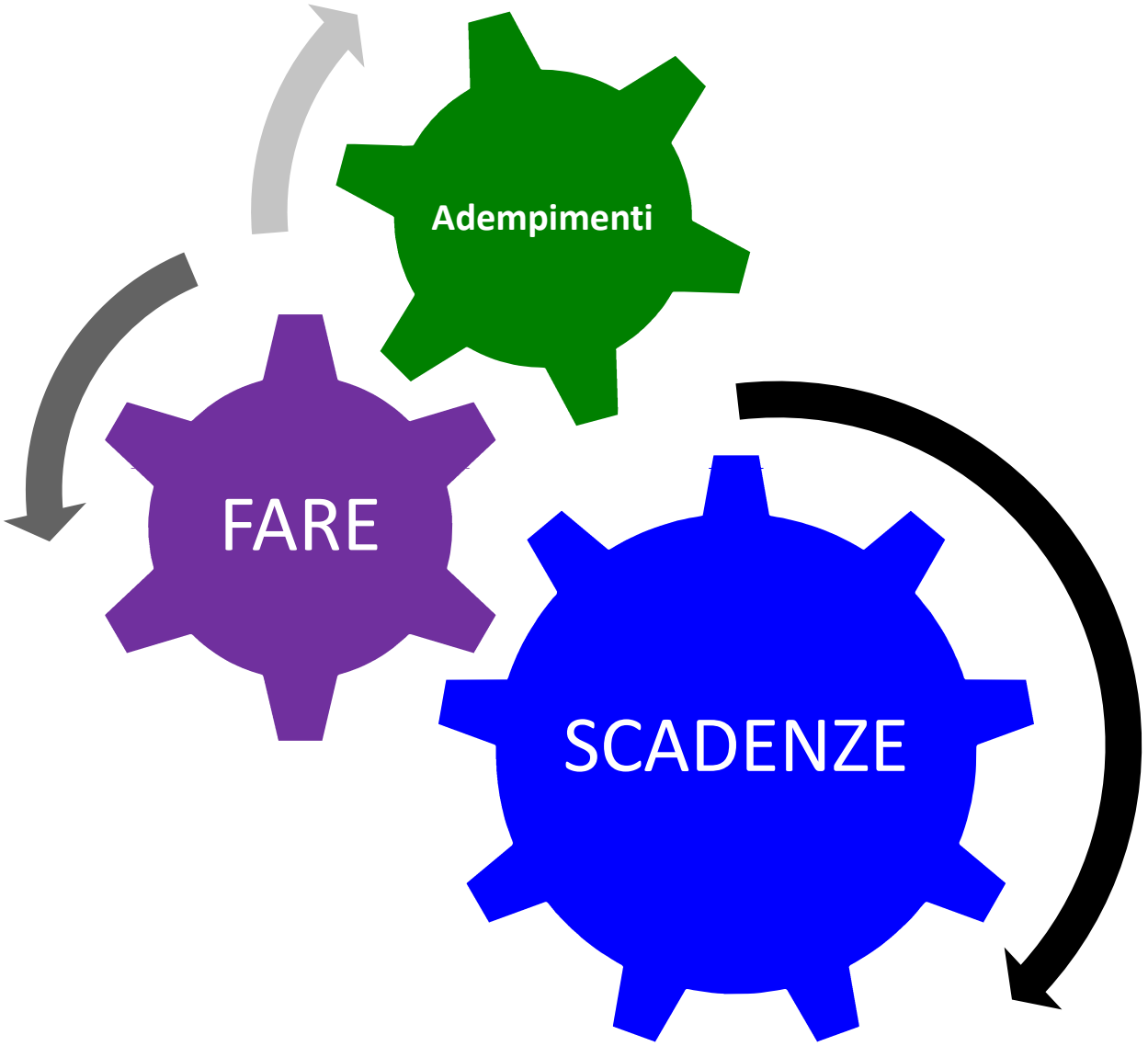
a. Digitalizzazione dei servizi amministrativi, gestionali e documentali; *software* e piattaforme per l'ufficio e il lavoro collaborativo; fatturazione elettronica; pagamenti elettronici (PagoPA);(8 ore)

b. Rendicontazione finanziaria; registri elettronici e archivi *cloud*; acquisti online e utilizzo delle piattaforme CONSIP e MEPA; amministrazione trasparente e obblighi di pubblicità; rendicontazione sociale, apertura e valorizzazione dei dati della scuola (open data); (12 ore)

Art.1 comma 58 legge 107/2015

Il Piano nazionale per la scuola digitale persegue i seguenti obiettivi:

1. realizzazione di attività volte allo **sviluppo delle competenze digitali degli studenti**,
2. **potenziamento degli strumenti didattici e laboratoriali** necessari a migliorare la formazione e i processi di innovazione delle istituzioni scolastiche;
3. **adozione di strumenti organizzativi e tecnologici per favorire la governance**, la trasparenza e la condivisione di dati, nonché lo scambio di informazioni tra dirigenti, docenti e studenti e tra istituzioni scolastiche ed educative e articolazioni amministrative del MIUR;
4. **formazione dei docenti per l'innovazione didattica e sviluppo della cultura digitale per l'insegnamento**, l'apprendimento e la formazione delle competenze lavorative, cognitive e sociali degli studenti;
5. **formazione dei direttori dei servizi generali e amministrativi, degli assistenti amministrativi e degli assistenti tecnici** per l'innovazione digitale nell'amministrazione;
6. **potenziamento delle infrastrutture di rete** con particolare riferimento alla connettività nelle scuole;
7. **valorizzazione delle migliori esperienze delle istituzioni scolastiche** anche attraverso la promozione di una rete nazionale di centri di ricerca e di formazione;
8. **definizione dei criteri e delle finalità per l'adozione di testi didattici** in formato digitale e per la produzione e la diffusione di opere e materiali per la didattica, anche prodotti autonomamente dagli istituti scolastici.


Adempimenti
FARE
SCADENZE

La digitalizzazione

Processo qualificante di efficienza e di trasparenza delle amministrazioni pubbliche

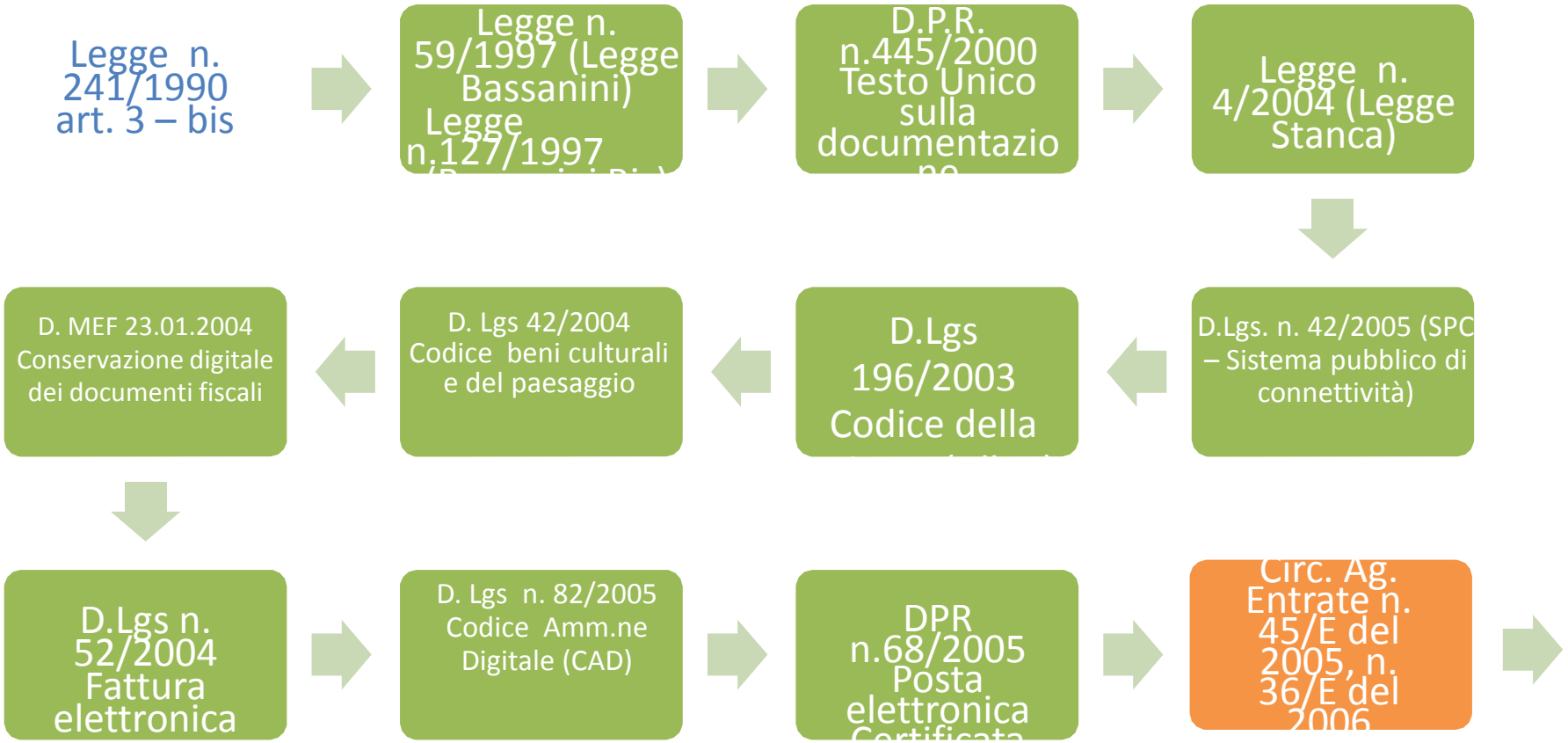
1. Risparmi diretti in termini di “carta e spazi recuperati” (inizio anni 2000);

2. Risparmi indiretti in termini di tempo ed efficacia dell'azione amministrativa pubblica, delle aziende e dei privati

Da quanto se ne parla?

Quali risultati sono stati raggiunti?

La digitalizzazione – prima del 2010



La digitalizzazione – dopo il 2010

La digitalizzazione: Risultati raggiunti ad oggi - Rapporto DESI 2015

Digital Economy and Society Index **(DESI) è l' Indice dell'Economia e della Società Digitale** della Commissione Europea (DG CNECT): traccia lo stato delle politiche digitali dei Paesi secondo una prospettiva più ampia di quella consentita dalla Digital Agenda Scoreboard.

Rapporto DESI 2015

25ˆ posto su 28

Con prestazioni inferiori alla media sono la Slovenia, Ungheria, Slovacchia, Cipro, Polonia che precedono l'Italia, e Grecia, Bulgaria e Romania che seguono l'Italia

La digitalizzazione: Risultati raggiunti ad oggi - Rapporto DESI 2015

Connettività : solo il 21% delle famiglie ha accesso a una connessione internet veloce (il livello di copertura più basso dell'UE), solo il 51% delle famiglie ha un abbonamento a banda larga fissa (la percentuale più bassa dell'UE)

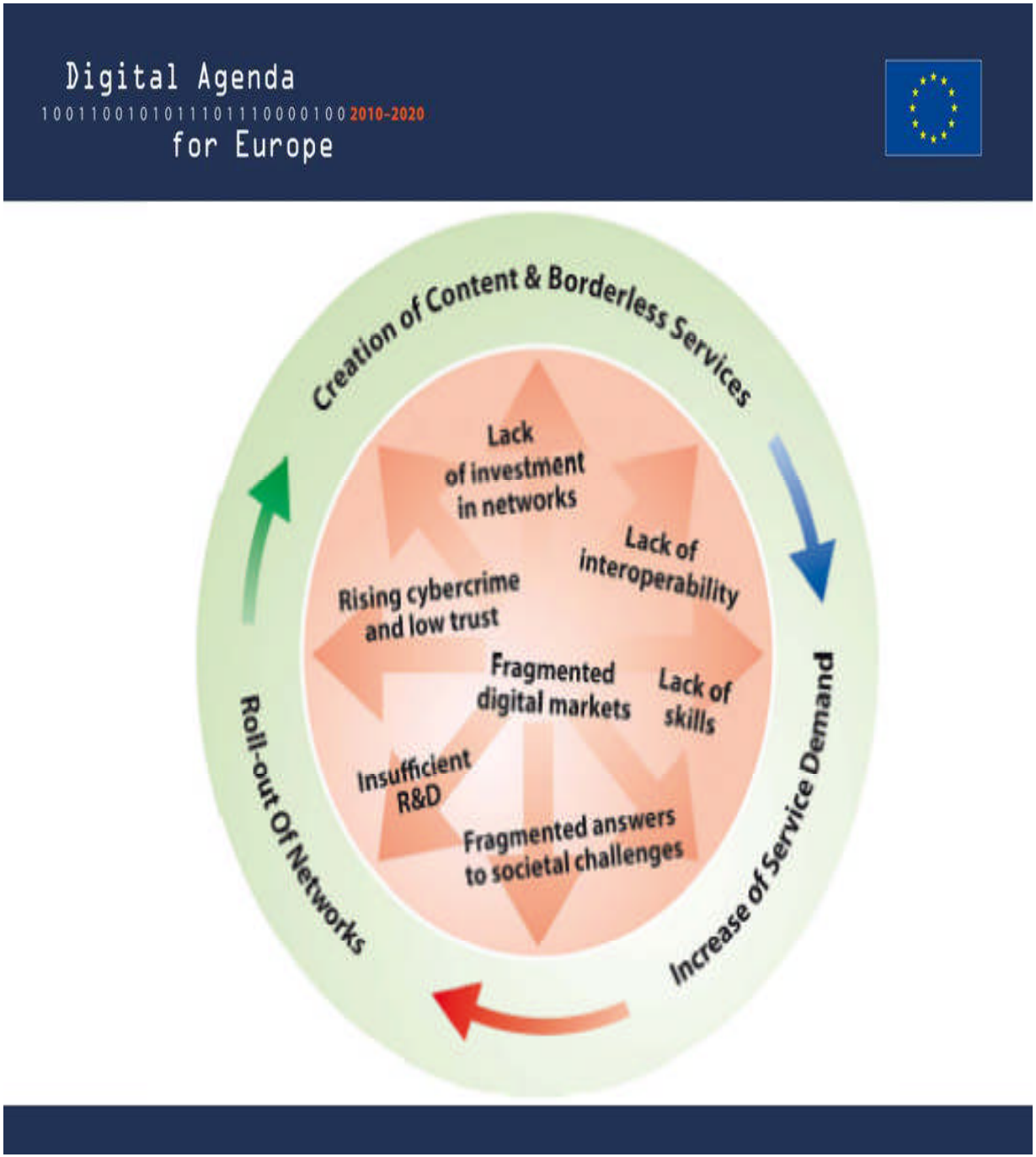
Domanda del Capitale Umano e dell'Uso di Internet : sviluppo dell'economia digitale sembra essere frenato dal basso livello di competenze digitali: solo il 59% degli utenti, una delle percentuali più basse dell'UE, usa abitualmente internet, mentre il 31% della popolazione italiana non lo ha mai utilizzato

PMI : solo il 5,1% delle PMI utilizza l'e-commerce, al quale è imputabile appena il 4,8% del fatturato complessivo delle imprese italiane, mentre il livello digitale dei processi produttivi e gestionali delle imprese di dimensione maggiore è ampiamente nella media europea;

Servizi pubblici digitali : l'Italia si avvicina complessivamente

L'agenda digitale si prefigge di generare crescita stimolando il "circolo virtuoso" ed eliminando le barriere a nuovi servizi e quindi all'**innovazione**, al fine di stimolare la domanda e aumentare incentivi agli investimenti in infrastrutture e alla nostra capacità di innovare.

In altre parole occorre far funzionare il circolo virtuoso.
Senza una strategia digitale non c'è strategia a lungo termine che tenga



Sono cittadino - Pubblicato il: 10/05/2012

Cosa puoi fare?

Se sei un genitore, comodamente da casa, via web, posta elettronica e sms, puoi:

1. iscrivere tuo figlio a scuola;
2. pagare le tasse scolastiche;
3. richiedere e ricevere documenti e certificati;
4. prenotare (o disdire) colloqui con i docenti;
5. consultare voti e pagelle;
6. ricevere avvisi su assenze e ritardi, e notifiche degli avvenimenti scolastici (uscite anticipate, chiusure programmate, consigli di istituto ed eventi culturali)

Se sei uno studente puoi, durante la tua degenza in ospedale e la post-degenza della malattia a casa:

- partecipare da remoto in tempo reale alle lezioni svolte in aula;
- visualizzare le lezioni registrate in ore e giorni precedenti;
- visionare in tempo reale un bouquet selezionato di canali televisivi di intrattenimento;
- dialogare con il mondo esterno attraverso strumenti di videocomunicazione interattiva.

Per approfondire:

ScuolaMia, il portale dei servizi online volti a favorire la comunicazione tra scuola e famiglie.

IoStudio - La Carta dello Studente, iniziativa che promuove l'accesso alla

Piano Nazionale Scuola Digitale (PNSD) - Strumenti

Accesso

- Priorità nel piano per la banda ultralarga: nel 2016 le prime coperture.
- Bando lan/wan realizzato cablaggio interno.
- A *marzo* ripartizione finanziamento di 10 milioni a supporto dei costi per la connettività (scuole non sostenute dalle amministrazioni).

Spazi e ambienti per l'apprendimento

- Ambienti per la didattica digitale (aule "aumentate", laboratori mobili, spazi alternativi) 4 mila scuole vincitrici finanziamento 100 milioni.
- "*Challenge prize*", progettazione di nuove soluzioni per la scuola digitale.
- Piano "laboratoriale", con i laboratori territoriali, gli atelier creativi e i laboratori professionalizzanti (bandi pubblicati a fine anno).

Identità digitale - In conformità al Sistema Pubblico di Identità Digitale (SPID), procedure di autenticazione ai sistemi Miur

Piano Nazionale Scuola Digitale (PNSD) - Strumenti

Amministrazione digitale.

1. Digitalizzazione delle procedure, partendo dall'adesione ai programmi nazionali (pagamenti elettronici).
2. Registro elettronico per tutte le scuole primarie.
3. Open data: Anagrafe dell'edilizia scolastica, Anagrafe degli studenti in forma aggregata, provvedimenti di incarico di docenza, POF triennali, Osservatorio tecnologico, Sistema nazionale di valutazione, bilanci delle scuole, materiali didattici e delle opere autoprodotte dagli istituti scolastici e rilasciati in formato aperto.

Piano Nazionale Scuola Digitale - Competenze

Competenze digitali.

1. Format innovativi di percorsi didattici, per rendere disponibili a tutti i docenti le migliori esperienze metodologiche già presenti.
2. Pensiero computazionale come "Programma il futuro".

Digitale, imprenditorialità e lavoro.

a. Bando costruzione di curricoli brevi per praticare l'imprenditorialità a scuola, oltre a diverse iniziative già avviate (olimpiadi imprenditorialità, *contamination labs, ..*).
b. Orientamento/raccordo strutturale tra scuola secondaria e università in campo tecnologico allo scopo di massimizzare gli apprendimenti degli studenti su competenze IT.

Contenuti digitali.

Bando per la costituzione di reti di scuole che completino o realizzino ex novo biblioteche scolastiche capaci di assumere anche la funzione di centri di documentazione e alfabetizzazione informativa, anche aperti al territorio circostante.

Piano Nazionale Scuola Digitale (PNSD) - Formazione

La formazione del personale.

1. Definiti gli snodi territoriali per l'erogazione della formazione, ripartizione delle risorse e quindi avvio delle attività.
2. Entro l'estate, avvio prima esperienza di alta formazione digitale, all'estero, presso i migliori centri e università del mondo, a 1.000 docenti e dirigenti scolastici con "forte propensione all'innovazione e alla cultura digitale".
3. A marzo tutte le istituzioni scolastiche del primo ciclo riceveranno una quota di 1.000 euro come parziale contributo per i costi di assistenza tecnica.

La formazione in ingresso per i neo-assunti.

Consolidamento pratiche di formazione innovativa per i neo-assunti (dalla progettazione online al peer-to-peer) che introducono all'utilizzo del digitale e alla sua applicazione nella didattica in modo da accompagnare i docenti nell'apprendimento.

Agenda digitale

Carta della cittadinanza digitale (Legge 124/2015 - Deleghe in materia di riorganizzazione delle p.a.

1. Definire un livello minimo dei diritti digitali degli utenti nei confronti di tutti i livelli amministrativi (possibilità di effettuare qualsiasi pratica/pagamento/ comunicazione in modalità telematica,ecc)
2. adeguare l'organizzazione delle amministrazioni alle sfide della digitalizzazione (ad es. ridefinire le competenze ed individuare un dirigente unico responsabile delle attività di digitalizzazione e agevolare la collaborazione tra le diverse amministrazioni, ecc);
3. Controllare diffusamente la p.a. con accesso gratuito ai dati anche senza un interesse diretto:"Freedom of information act" (FOIA), ossia il sistema generale di pubblicità e trasparenza, già radicato nei paesi anglosassoni.

integrare il pnsd al ptof

“La formazione degli insegnati può favorire un migliore utilizzo degli strumenti Ict a scuola; il loro uso, per essere efficace, deve essere guidato dal **solo obiettivo di migliorare l'apprendimento degli studenti.** Non bisogna pensare alle tecnologie digitali come qualcosa di distinto dagli altri aspetti della pratica didattica, ma vedere come le competenze digitali si legano a tutte le altre. Le nuove tecnologie da sole non risolvono i problemi, ma possono aiutare a cambiare.” F. Avvisati ricercatore OCSE

Obiettivi formativi prioritari studenti(art. 1 comma 7 legge 107/2015):
h) sviluppo delle competenze digitali degli studenti, con particolare riguardo al pensiero computazionale, all'utilizzo critico e consapevole dei social network e dei media nonché alla produzione e ai legami con il mondo del lavoro;
i) potenziamento delle metodologie laboratoriali e delle attività di laboratorio.

Criticità ???

a) Dirigenti scolastici e, anche se in misura minore, direttori amministrativi sono cruciali per PNSD: parte attiva/ positiva del cambiamento e l'accompagnamento (formazione, coaching, tutorship, ma anche di obiettivi chiari e valutazioni coerenti);

b) Il Piano di Miglioramento, derivante dal RAV ora pubblico, è l'innesco delle innovazioni del PNSD rispetto a carenze e specificità di ogni singola scuola. Perciò RAV, PNSD, PdM, POF triennale … ma è chiaro??

c) *Comunicare la visione - Rimuovere gli ostacoli* necessita di supporto. A chi sarà in carico? Alle reti di scuole? A Indire sul miglioramento? Quando sarà definito?

d) Chi deve governare il cambiamento: USR, reti, AgiD …

e) … i cambiamenti si realizzano se il valore dell'innovazione viene affermato inequivocabilmente da chi lo promuove, e quindi, anche, se viene premiato chi innova e disincentivato chi resiste …

Piano Nazionale Scuola Digitale (PNSD) -Tavoli tecnici

a) BYOD (Bring Your Own Device) e linee guida: indirizzare scelte tecniche per consentire agli studenti di utilizzare i propri dispositivi (AgID);
b) framework per le competenze digitali degli studenti, anche proponendo una revisione delle indicazioni nazionali;
c) aggiornamento del curricolo di "Tecnologia" alla secondaria di primo grado;
d) standard minimi/requisiti tecnici per gli ambienti on line per la didattica, in collaborazione con AgID;
e) definizione di linee guida per l'autoproduzione di contenuti didattici digitali;
f) contenuti della formazione in servizio per innovazione didattica e organizzativa.

ACCOMPAGNAMENTO

- Un animatore digitale in ogni scuola
- Accordi territoriali
- Stakeholders' Club per la scuola digitale
- Un galleria per la raccolta di pratiche
- Dare alle reti innovative un ascolto permanente
- Osservatorio per la Scuola Digitale
- Un comitato Scientifico che allinei il Piano alle pratiche internazionali
- Il monitoraggio dell'intero Piano
- Un legame palese con il Piano Triennale per l'Offerta Formativa

Le "principali novità" con relative scadenze

Norma di riferimento	Ambito	In Vigore	Adeguamento
DPCM 3 dicembre 2013 – Regole tecniche per il protocollo informatico ai sensi degli articolo 40-bis, 41, 47, 57-bis e 71 del CAD di cui al d.l.n.82 del 2005	Protocollo Informatico	Pubblicato in GU il 12 marzo 2014 entrato in vigore il 12 aprile 2014	**Entro il 12 ottobre 2015**
Regolamento UE n. 910/2014 del Parlamento Europeo e del Consiglio in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno e che abroga la direttiva 1999/93/CE	Firme elettroniche, sigilli	Adottato in CE il 23 luglio 2014, Pubblicato in GU UE il 28 agosto 2014 entrato in vigore il 17 settembre 2014	**Entro il 1 luglio 2016**
DPCM 13 novembre 2014 – Regole tecniche in materia di formazione, trasmissione, copia, duplicazione, riproduzione e validazione temporale dei documenti informatici, nonché di formazione e conservazione dei documenti informatici delle Pubbliche Amministrazione ai sensi degli articoli 20, 22, 23-bis, 23-ter, 40 comma 1, 41 e 71 comma 1, del CAD di cui al d.l.n.82 del 2005	Documento Informatico	Pubblicato in GU il 12 gennaio 2015, entrato in vigore il 12 febbraio 2015	**Entro il 12 agosto 2016**
DPCM 3 dicembre 2013 – Regole tecniche in materia di sistema di conservazione ai sensi degli articoli 20 commi 3 e 5-bis, 23- ter comma 4, 43 commi 1 e 3, 44, 44-bis e 71 comma 1 del CAD di cui al d.l. n.82 del 2005	Conservazione a lungo termine	Pubblicato in GU il 12 marzio 2014 entrato in vigore il 12 aprile 2014	**Entro il 12 aprile 2017**

BIG DATA @MIUR

RAPPORTO DEL GRUPPO DI LAVORO

Struttura e fruibilità dei dati MIUR

- Il rapporto ha mappato il sistema informativo del MIUR, organizzato nei tre sottosistemi dell'***ISTRUZIONE*** dell'***UNIVERSITÀ*** e della ***RICERCA***, le loro macro-aree e i processi e dati connessi.

- Il patrimonio di informazioni del MIUR può essere classificato sulla base dei soggetti a cui le stesse si riferiscono. Si possono individuare **tre principali categorie:**

1.singole istituzioni (scuole, università, enti di ricerca e altre istituzioni di alta formazione): informazioni sulle strutture, sull'offerta formativa, sulle risorse economiche e umane, sulla produzione scientifica e quelle derivanti dalle attività di autovalutazione e valutazione;

2.studenti: informazioni relative al percorso formativo e ai principali eventi nella carriera scolastica e universitaria;

3.personale **docente e amministrativo**: informazioni sul percorso professionale e sul trattamento economico, ma anche, in maniera eterogenea per le diverse carriere, sulla produzione scientifica, sugli incarichi ricoperti e la formazione.

Struttura e fruibilità dei dati MIUR

L'autonomia che contraddistingue i diversi comparti ha contribuito allo sviluppo di distinte modalità di gestione delle informazioni, generando **un'eterogeneità di *repository* poco comunicanti** tra loro.
Le informazioni sono già oggi utilizzate per la formulazione delle politiche e per l'analisi dei sistemi scolastico, universitario e della ricerca. Sono anche in parte a disposizione delle singole istituzioni per le loro scelte gestionali e al più ampio pubblico attraverso dei portali dedicati.

Il Ministero è però oggi nelle condizioni di compiere un **salto qualitativo in ottica Big Data e implementare una strategia di sistematica valorizzazione e integrazione del proprio patrimonio informativo**

Una strategia Big Data per il MIUR

- **Aumentare la capacità** di governare, sia dal punto di vista gestionale sia analitico, queste immense moli di informazioni
  - ➢ implementare un ambiente ministeriale (virtualmente) centralizzato di *data e content management*
  - ➢ garantire la interoperabilità dei diversi data base, indipendentemente dai processi amministrativi da cui originano, delle amministrazioni a cui si riferiscono, dei sistemi gestionali adottati
  - ➢ consolidare i dati ed eliminare le ridondanze
- **Integrare/arricchire le informazioni** con dati provenienti da **altre amministrazioni** (Ministero del Lavoro, Istat, Inail, etc.)
- Integrare/arricchire le informazioni sfruttando in una logica Big Data anche le informazioni liberamente ricavabili dal **web e dai social network**
- **Diffondere** in formato aperto i dati, ferma restando l'esigenza di assicurare i necessari **profili di privacy**

Privacy: informativa

d.lgs.30.06.2003, n. 196 - Codice in materia di protezione dei dati personali

Chi intende effettuare un trattamento di dati personali deve **prima** fornire all'interessato alcune informazioni *(art. 13 Codice)* per metterlo nelle condizioni di esercitare i propri diritti *(art. 7 Codice)*.

In particolare, l'informativa deve spiegare:

1. in che modo e per quale scopo verranno trattati i propri dati personali;
2. se il conferimento dei propri dati personali è obbligatorio o facoltativo;
3. le conseguenze di un eventuale rifiuto a rendere disponibili i propri dati personali;
4. a chi saranno comunicati o se saranno diffusi i propri dati personali;
5. i diritti previsti dall' *art. 7* del Codice;
6. chi è il titolare e (se è stato designato) il responsabile del trattamento.

Se i dati personali sono stati raccolti da altre fonti (*ad esempio*, archivi pubblici, familiari dell'interessato, ecc.), cioè non direttamente presso l'interessato, l'informativa deve essere resa:

- quando i dati sono registrati

oppure

- non oltre la prima comunicazione a terzi

L'omessa o inidonea informativa è punita con la sanzione amministrativa del pagamento di una somma da seimila euro a trentaseimila euro *(art.161del Codice)*.

Privacy: consenso

Soggetti privati e enti pubblici economici

Per i soggetti privati e gli enti pubblici economici il trattamento di dati personali è possibile con il **consenso** dell'interessato documentato per iscritto *(articolo 23 del Codice)*, che è valido se:

- ✓all'interessato è stata resa l'**informativa** *(articolo 13 del Codice)*;
- ✓è stato espresso dall'interessato liberamente e specificamente in riferimento ad un trattamento chiaramente individuato (oppure a singole operazioni di trattamento).

Soggetti pubblici

Le pubbliche amministrazioni non devono richiedere il consenso dell'interessato, purché il trattamento sia effettuato nell'ambito dello svolgimento delle proprie funzioni istituzionali *(articolo 18 del Codice)*.

Il trattamento di dati personali effettuato in violazione dell'*articolo 23* ***del Codice è punito con la sanzione amministrativa del pagamento di una somma da diecimila euro a centoventimila euro*** *(articolo 162, comma 2 bis* ***del Codice).***

Privacy: modalità di trattamento

Il trattamento deve avvenire riducendo al minimo l'utilizzo di dati personali *(principio di necessità - articolo 3 del Codice)*, oltre che nel rispetto dei seguenti principi *(articolo 11del Codice)*:

a. liceità e correttezza del trattamento;
b. finalità del trattamento;
c. esattezza e aggiornamento dei dati;
d. pertinenza, completezza e non eccedenza dei dati raccolti rispetto alle finalità del trattamento;
e. conservazione dei dati per un tempo non superiore a quello necessario rispetto agli scopi per i quali è stato effettuato il trattamento.

Privacy: trattamento di dati sensibili e giudiziari

Soggetti privati e enti pubblici economici

I soggeti privati e gli enti pubblici economici possono effettuare un trattamento di:
- dati sensibili con il consenso scritto dell'interessato e previa **autorizzazione** del Garante per la protezione dei dati personali *(articolo 26 del Codice)*, salvo alcune eccezioni specificamente previste;
- dati giudiziari se autorizzati da una espressa disposizione di legge o da un provvedimento del Garante per la protezione dei dati personali *(articolo 27 del Codice)*.

Soggetti pubblici

Le pubbliche amministrazioni possono effettuare un trattamento di dati sensibili e dati giudiziari sulla base delle disposizioni specifiche previste dagli articoli 20, 21 e 22 *del Codice in materia di protezione dei dati personali*.

Privacy: trasferimento dei dati all'estero

Verso Paesi appartenenti all'Unione europea

Le legislazioni dei Paesi aderenti all'Unione europea (adottate in attuazione della *direttiva comunitaria 95/46/CE)* sono considerate equivalenti in relazione all'adeguata tutela in materia di protezione dei dati personali. Il trasferimento attraverso o verso questi Paesi non è quindi soggetto a particolari restrizioni *(articolo 42 del Codice)*.

Verso Paesi non appartenenti all'Unione europea

Il trasferimento di dati personali verso Paesi non appartenenti all'Unione europea è possibile **quando**:

- ricorre una delle condizioni previste dall' *articolo 43* del Codice in materia di protezione dei dati personali - oppure, è autorizzato dal Garante per la protezione dei dati personali sulla base di adeguate garanzie per i diritti dell'interessato *(articolo 44 del Codice)*

Fuori da questi casi, il trasferimento è vietato quando l'ordinamento del Paese di destinazione o di transito dei dati personali non assicura un livello adeguato di tutela delle persone *(articolo 45 del Codice)*.

Il trasferimento di dati personali effettuato in violazione dell'articolo 45 del Codice è punito con la sanzione amministrativa del pagamento di una somma da diecimila euro a centoventimila euro *(articolo 162 comma 2 bis del Codice)*.

Privacy: cessazione del trattamento

In caso di cessazione del trattamento, i dati personali devono essere *(articolo 16 del Codice)*:

a) distrutti;
b) ceduti ad altro titolare, purchè destinati ad un trattamento in termini compatibili agli scopi per i quali i dati sono raccolti;
c) conservati per fini esclusivamente personali e non destinati ad una comunicazione sistematica o alla diffusione;
d) conservati o ceduti ad altro titolare per scopi storici, statistici o scientifici.

Privacy: misure di sicurezza

Il titolare del trattamento è obbligato ad adottare misure di sicurezza idonee a ridurre al minimo i rischi di distruzione, perdita, accesso non autorizzato o trattamento dei dati personali non consentito o non conforme alle finalità della raccolta *(articolo 31 del Codice)*.

In particolare, il titolare deve adottare le **misure minime di sicurezza** *(articolo 33 del Codice e Allegato B al Codice)* volte ad assicurare un livello minimo di protezione dei dati personali.

Privacy: misure di sicurezza

La sicurezza informatica equivale quindi ad attuare tutte le misure e tutte le tecniche necessarie per proteggere l'hardware, il software ed i dati dagli accessi non autorizzati (intenzionali o meno), per garantirne la riservatezza, nonché eventuali usi illeciti, dalla divulgazione, modifica e distruzione.

L'omessa applicazione delle misure minime di sicurezza è punita con la sanzione amministrativa del pagamento di una somma da diecimila euro a centoventimila euro (*articolo 162, comma 2 bis****del Codice) e con la sanzione penale dell'arresto fino a 2 anni (****articolo 169 ****del Codice)*****.**

Privacy: misure di sicurezza per i trattamenti con strumenti elettronici

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

a) autenticazione informatica;
b) adozione di procedure di gestione delle credenziali di autenticazione;
c) utilizzazione di un sistema di autorizzazione;
d) aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici;
e) protezione degli strumenti elettronici e dei dati rispetto a trattamenti illeciti di dati, ad accessi non consentiti e a determinati programmi informatici;
f) adozione di procedure per la custodia di copie di sicurezza, il ripristino della disponibilità dei dati e dei sistemi;
g) adozione di tecniche di cifratura o di codici identificativi per determinati trattamenti di dati idonei a rivelare lo stato di salute o la vita sessuale effettuati da organismi sanitari.

Privacy: misure di sicurezza per i trattamenti senza l'ausilio di strumenti elettronici

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

a) aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unità organizzative;
b) previsione di procedure per un'idonea custodia di atti e documenti affidati agli incaricati per lo svolgimento dei relativi compiti;
c) previsione di procedure per la conservazione di determinati atti in archivi ad accesso selezionato e disciplina delle modalità di accesso finalizzata all'identificazione degli incaricati.

Fiducia e sicurezza online

furti d'identità
cyber-criminalità

pericoli per la privacy
spam

Centro per la criminalità informatica

- **Squadre di pronto intervento informatico**
- **Aggiornamento** della direttiva sulla **privacy**

Fiducia e sicurezza online

Rapporto Clusit 2016 (Associazione Italiana per la Sicurezza Informatica):

1. confermano ed una crescita anche in Italia degli attacchi; ben il + 30% rispetto al 2015 è riconducibile a fenomeni di cyber crime con apparenti finalità criminali;

2. evidenziano modalità di attuazione degli attacchi evolute, passando ad attacchi più ampi, finalizzati ad ottenere risultati di medio-lungo periodo che coinvolgono anche il governo delle nuove tecnologie ICT. Ad esempio attacchi ai social media o ai servizi in cloud, così come il controllo degli oggetti connessi ad internet, IoT o relativi agli apparati di controllo industriale – c.d. SCADA – per le infrastrutture critiche coinvolte nell'erogazione di servizi primari per il Paese – quali Acqua, Energia, Trasporti.

3. Sottolineano la necessità di sensibilizzare la Pubblica Amministrazione a dotarsi d'infrastrutture, processi e competenze per gestire la sicurezza IT.

Fiducia e sicurezza online
Impact Analisys: minacce

Infrastrutture fisiche/logiche che concorrono a determinare l'attività dell'ente/azienda l'ubicazione geografica del sito dove risiedono le macchine principali ha la stessa valenza della gestione e della conoscenza degli apparati Hw e Sw gestiti.
Comunicazioni Le comunicazioni rispetto alla gestione delle minacce deve essere monitorato costantemente e la formazione in tal senso deve essere uno degli asset preventivi che l'ente/azienda devono sempre tener presente. Non si potrà mai intervenire, nemmeno in presenza di un ottimo piano di ***Disaster Ricovery (DR)***se le risorse coinvolte non hanno ricevuto le giuste comunicazioni e la giusta formazione per intervenire.
Personale L'identificazione del personale coinvolto deve essere chiara e non presentare ambiguità sulla responsabilità delle singole azioni.
Fornitori I fornitori devono essere scelti anche in funzioni delle attività che devono svolgere a fronte di un evento che alteri il normale stato delle cose. Il fornitore va valutato anche in considerazione del fatto che all'atto dell'installazione di un qualsiasi prodotto abbia anche presentato un paino di interventi e di modifiche compliance con il piano di DR

Fiducia e sicurezza online
Impact Analisys: minacce

Utilities La scelta di utilities da approntare su un paino di DR è fondamentale: vanno quindi monitorate nell'utilizzo per verificarne le risposte e l'attendibilità in casi al critici.

Documentazione il recupero della documentazione rappresenta un attività fortemente pericolosa anche perché si parte quasi sempre da documentazione obsoleta. Occorre invece raccogliere, catalogare e rendere attuali tutti i documenti che riguardano ad esempio l'infrastruttura come possono essere i diagrammi di rete, i data- base, le licenze delle applicazioni e le configurazione dei dispositivi ma si potrebbe continuare.

Sistemi informativi rappresentano la prima e più importante attività di studio propedeutica alla gestione del DR; si tenga presente che i sistemi informativi vanno soggetti a continui aggiornamenti e quindi rappresentano un continuo cambio nell'operatività del Piano. Un aggiornamento non eseguito o addirittura eseguito senza tener presente regole/policy dell'ente/azienda possono generare un elemento critico dal quale diventa arduo uscirne.

Apparati hardware Vale quanto già detto precedentemente per le infrastrutture e per i fornitori.

Siti geografici E necessario conoscere perfettamente la realtà geografica nella quale è posta un sito sia esso primario o secondario, perché solo così il piano

Fiducia e sicurezza online: il nuovo CAD: la trasformazione annunciata 1/2

… individuare strumenti per definire il livello minimo di sicurezza, qualità, fruibilità, accessibilità e tempestività dei servizi on line; prevedere speciali regimi sanzionatori e premiali per p.a.;

… ridefinire e semplificare i procedimenti amministrativi, in relazione alle esigenze di celerità, certezza dei tempi e trasparenza per cittadini/imprese, mediante digitalizzazione e realizzazione del principio "digital first"(innanzitutto digitale), nonchè l'organizzazione /procedure interne;

… garantire, in linea con gli obiettivi dell'Agenda Digitale Europea, connettività a banda larga e ultralarga e l'accesso a internet presso gli uffici pubblici, anche attribuendo carattere prioritario nei bandi all'infrastrutturazione nei settori scolastico, sanitario e turistico (wi-fi unico ad accesso libero, con autenticazione tramite SPID, presente in tutti i luoghi di particolare interesse turistico)

Fiducia e sicurezza online: il nuovo CAD: la trasformazione annunciata 2/2

… garantire l'**accesso** e il **riuso** gratuiti di tutte le informazioni prodotte/detenute dalle p.a. in formato aperto, l'alfabetizzazione digitale, la **partecipazione** con modalità **telematiche** ai **processi decisionali** delle p.a., la piena disponibilità dei sistemi di pagamento elettronico nonchè la riduzione del divario digitale sviluppando le competenze digitali di base;

… razionalizzare i meccanismi/strutture deputati alla **governance della digitalizzazione**, al fine di semplificare i processi decisionali;

… **adeguare le disposizioni vigenti a quelle europee**, per garantire la coerenza giuridica, logica e sistematica della normativa e per adeguare, aggiornare e semplificare il linguaggio normativo e coordinare le discipline speciali con i princìpi del CAD;

… i **pagamenti digitali/elettronici** effettuati con qualsiasi modalità di pagamento, ivi incluso l'utilizzo per i micropagamenti del credito telefonico, costituiscano il mezzo principale per i pagamenti verso p.a. e degli esercenti servizi di pubblica utilità.

Regolamento europeo in materia di protezione dei dati personali
(24 maggio 2016 / 25 maggio 2018)

Il **4 maggio 2016**, sono stati pubblicati sulla Gazzetta Ufficiale dell'Unione Europea (GUUE) i testi del Regolamento europeo in materia di protezione dei dati personali e della Direttiva che regola i trattamenti di dati personali nei settori di prevenzione, contrasto e repressione dei crimini.
Il **5 maggio 2016** è entrata ufficialmente in vigore la Direttiva, che dovrà essere recepita dagli Stati membri entro 2 anni.
Il **24 maggio 2016** è entrato ufficialmente in vigore il Regolamento, che diventerà definitivamente applicabile in via diretta in tutti i Paesi UE a partire dal **25 maggio 2018**.

Cittadini più garantiti

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

Informazioni più chiare e complete sul trattamento

L'informativa diventa sempre di più uno strumento di trasparenza riguardo al trattamento dei dati personali e all'esercizio dei diritti.

Per facilitare la comprensione dei contenuti, nell'informativa si potrà fare ricorso anche a icone, identiche in tutta l'Unione europea.

Gli interessati dovranno sapere se i loro dati sono trasmessi al di fuori dell'Ue e con quali garanzie; cosi come dovranno sapere che hanno il diritto di revocare il consenso a determinati trattamenti, come quelli a fini di marketing diretto.

Consenso, strumento di garanzia anche on line

Il consenso dell'interessato al trattamento dei dati personali dovrà essere, come oggi, preventivo e inequivocabile, anche quando espresso attraverso mezzi elettronici (ad esempio, selezionando un'apposita casella in un sito web).

Per trattare i dati sensibili, il Regolamento prevede che il consenso deve essere anche «esplicito».

Il consenso potrà essere revocato in ogni momento.

I trattamenti effettuati fino a quel momento dal titolare sulla base del consenso rimarranno comunque legittimi.

Viene esclusa ogni forma di consenso tacito (il silenzio, cioè, non equivale al consenso) oppure ottenuto proponendo a un interessato una serie di opzioni già selezionate.

I fornitori di servizi Internet e i social media, dovranno richiedere il consenso ai genitori o a chi esercita la potestà genitoriale per trattare i dati personali dei minori di 16 anni.

Limiti alla possibilità per il titolare di adottare decisioni solo sulla base di un trattamento automatizzato di dati

Le decisioni che producono effetti giuridici (come, la concessione di un prestito) non potranno essere basate esclusivamente sul trattamento automatizzato dei dati (ad esempio, la profilazione).

Faranno eccezione i casi in cui l'interessato abbia rilasciato un consenso esplicito al trattamento automatizzato dei suoi dati, oppure questo tipo di trattamento risulti strettamente necessario per la definizione di un contratto o avvenga in base a specifici obblighi di legge.

In ogni caso, sono previste garanzie per gli interessati, come il diritto di opporsi alla decisione adottata sulla base di un trattamento automatizzato o il diritto di ottenere anche l'intervento umano rispetto alla decisione stessa.

Se il trattamento è finalizzato ad attività di marketing diretto, l'interessato ha sempre il diritto di opporsi alla profilazione.

Più tutele e libertà con il diritto all'oblio

Grazie all'introduzione del cosiddetto «diritto all'oblio», gli interessati potranno ottenere la cancellazione dei propri dati personali anche on line da parte del titolare del trattamento qualora ricorrano alcune condizioni previste dal Regolamento: se i dati sono trattati solo sulla base del consenso; se i dati non sono più necessari per gli scopi rispetto ai quali sono stati raccolti; se i dati sono trattati illecitamente; oppure se l'interessato si oppone legittimamente al loro trattamento.

A questo diritto si accompagna l'obbligo per il titolare del trattamento che ha pubblicato i dati di comunicare la richiesta di cancellazione a chiunque li stia trattando, nei limiti di quanto tecnicamente possibile.

Il diritto all'oblio potrà essere limitato solo in alcuni casi specifici: per esempio, per garantire l'esercizio della libertà di espressione o il diritto alla difesa in sede giudiziaria; per tutelare un interesse generale (ad es., la salute pubblica); oppure quando i dati, resi anonimi, sono necessari per la ricerca storica o per finalità statistiche o scientifiche.

Portabilità dei dati: liberi di trasferire i propri dati in un mercato digitale più aperto alla concorrenza

Il Regolamento introduce il diritto alla «portabilità» dei propri dati personali per trasferirli da un titolare del trattamento ad un altro.

Ad esempio, si potrà cambiare il *provider* di posta elettronica senza perdere i contatti e i messaggi salvati.

Ci saranno però alcune eccezioni che non consentono l'esercizio del diritto:
in particolare, quando si tratta di dati contenuti in archivi di interesse pubblico, come ad esempio le anagrafi.

Garanzie rigorose per il trasferimento dei dati al di fuori dell'Ue

Resta vietato il trasferimento di dati personali verso Paesi situati al di fuori dell'Unione europea o organizzazioni internazionali che non rispondono agli standard di adeguatezza in materia di tutela dei dati, rispetto ai quali il Regolamento introduce criteri di valutazione più stringenti.

Come avviene già oggi, in mancanza di un riconoscimento di adeguatezza da parte della Commissione europea, i titolari potranno utilizzare per il trasferimento specifiche garanzie contrattuali, per le quali il Regolamento prevede norme dettagliate e vincolanti.

In assenza di garanzie contrattuali o riconoscimenti di adeguatezza,

i dati potranno essere trasferiti solo con il consenso esplicito dell'interessato, oppure qualora ricorrano particolari condizioni

(ad esempio, quando il trasferimento è indispensabile per rispettare specifici obblighi contrattuali, per importanti motivi di interesse pubblico, per esercitare o difendere un diritto in sede giudiziaria, ecc.).

Il trasferimento o la comunicazione di dati personali di un cittadino dell'Ue ad autorità giudiziarie o amministrative di Paesi terzi potranno avvenire solo sulla base di accordi internazionali di mutua assistenza giudiziaria o attraverso strumenti analoghi.

Obbligo di comunicare i casi di violazione dei dati personali *(data breach)*

Il titolare del trattamento dovrà comunicare eventuali violazioni dei dati personali (*data breach*) all'Autorità nazionale di protezione dei dati.

Se la violazione dei dati rappresenta una minaccia per i diritti e le libertà delle persone, il titolare dovrà informare in modo chiaro, semplice e immediato anche tutti gli interessati e offrire indicazioni su come intende limitare le possibili conseguenze negative.

Il titolare del trattamento potrà decidere di non informare gli interessati se riterrà che la violazione non comporti un rischio elevato per i loro diritti (quando non si tratti, ad esempio, di frode, furto di identità, danno di immagine, ecc.); oppure se dimostrerà di avere adottato misure di sicurezza (come la cifratura) a tutela dei dati violati; oppure, infine, nell'eventualità in cui informare gli interessati potrebbe comportare uno sforzo sproporzionato (ad esempio, se il numero delle persone coinvolte è elevato).

In questo ultimo caso, è comunque richiesta una comunicazione pubblica o adatta a raggiungere quanti più interessati possibile (ad esempio, tramite un inserzione su un quotidiano/comunicazione sul sito web del titolare).

L'Autorità di protezione dei dati potrà comunque imporre al titolare del trattamento di informare gli interessati sulla base di una propria autonoma valutazione del rischio associato alla violazione.

Le novità per le imprese e gli enti

Imprese ed enti avranno più responsabilità, ma potranno beneficiare di semplificazioni.
In caso di inosservanza delle regole sono previste sanzioni, anche elevate.

Un unico insieme di norme per tutti gli Stati dell'Unione europea

Il Regolamento è direttamente applicabile e vincolante in tutti gli Stati membri dell'Unione europea e non richiede una legge di recepimento nazionale.

Inoltre, si applica integralmente alle imprese situate fuori dall'Unione europea che offrono servizi o prodotti a persone che si trovano nel territorio dell'Unione europea.

Tutte le aziende, ovunque stabilite, dovranno quindi rispettare le regole fissate nell'Ue.

Fra le principali novità del Regolamento c'è il cosiddetto «sportello unico» (*one stop shop*), che semplificherà la gestione dei trattamenti e garantirà un approccio uniforme.

Salvo casi specifici, le imprese stabilite in più Stati membri o che offrono prodotti e servizi in vari Paesi dell'Ue, per risolvere possibili problematiche sull'applicazione e il rispetto del Regolamento potranno rivolgersi ad un solo interlocutore: cioè all'Autorità di protezione dei dati del Paese dove si trova il loro stabilimento principale.

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».

Semplificazioni per i soggetti che offrono maggiori garanzie e promuovono sistemi di autoregolamentazione

Il Regolamento promuove il ricorso a codici di condotta da parte di associazioni di categoria e altri soggetti, sottoposti all'approvazione dell'Autorità nazionale di protezione dei dati ed eventualmente della Commissione europea (nel caso dell'approvazione da parte della Commissione il codice di condotta avrà applicazione nell'intera Ue).

Il titolare potrà far certificare i propri trattamenti, in misura parziale o totale, anche ai fini di trasferimenti di dati in Paesi terzi.

La certificazione potrà essere rilasciata da un soggetto abilitato oppure dall'Autorità di protezione dei dati.

L'adesione ai codici di condotta e la certificazione dei trattamenti saranno elementi di cui l'Autorità dovrà tenere conto, per esempio, nell'applicare eventuali sanzioni o nell'analizzare la correttezza di una valutazione di impatto effettuata dal titolare.

Il Regolamento punta a rispondere alle sfide poste dagli sviluppi tecnologici e dai nuovi modelli di crescita economica, tenendo conto delle esigenze di tutela dei dati personali sempre più avvertite dai cittadini dei Paesi dell'Unione europea.

Projectwork (I parte)

Proposta laboratoriale (I parte)

1. Favorire la formazione di gruppi eterogenei per competenze digitali

2. In ogni gruppo, ciascuno considera la procedura di protocollazione e pubblicazione legale e segnala:

- almeno un punto di positività in termini di processo di digitalizzazione

-almeno un punto di criticità in termini di processo di digitalizzazione

3. Si raccolgono le idee su post-it provenienti dai diversi gruppi

4. Discussione finale

Projectwork (II parte)

Proposta laboratoriale (II parte)

- si riprendono i punti di criticità e si individua una soluzione che possa trovare concreta applicazione
- trasformare la soluzione proposta in percorso progettuale
- evidenziare le componenti necessarie in termini di risorse materiali e UMANE.
    - già disponibili
    - opinabili ma non indispensabili
    - mandatorie

PRODOTTO FINALE (PROJECT WORK) in forma di mappa concettuale, presentazione, o altro...