

Diritto informatico semplice (per davvero)

Rovesti Gabriel

Attenzione



Il file non ha alcuna pretesa di correttezza; di fatto, è una riscrittura attenta di appunti, slide, materiale sparso in rete, approfondimenti personali dettagliati al meglio delle mie capacità. Credo comunque che, per scopo didattico e di piacere di imparare (sì, io studio per quello e non solo per l'esame) questo file possa essere utile. Semplice si pone, per davvero ci prova.

Thank me sometimes, it won't kill you that much.

Gabriel

Sommario

Diritto privato: definizione, fonti, soggetti, regolamenti (inizio parte Viglione).....	3
Decreti, applicazione norme, interpretazione, risoluzione conflitti.....	5
Contratti digitali: disciplina generale, stipula, terminologie	6
Contratti digitali: clausole/reso/diritti vari.....	8
Contratti digitali: controversie e smart contracts. Diritto dei beni: introduzione	11
Diritto d'autore, Successione nel patrimonio digitale.....	13
Responsabilità civile	15
Lavoro e tecnologia (inizio parte Sitzia)	18
Protezione e tutela dell'individuo in ambito reale (fine Decent Work by Design).....	20
Subordinazione/autonomia.....	21
Controversie individuali e potere direttivo (lavoro subordinato)	22
Potere disciplinare e diritti sindacali	24
Diritto del lavoro: lavoro e persona	26
Lavoro, persone e tecnologie	28
Strumenti di lavoro e accordi/vincoli nel loro utilizzo.....	29
Privacy (inizio parte Ruggiu)	32
Discorso generale sulla privacy e sul ruolo del GDPR.....	33
Privacy e profili generali regolamento UE	35
Questioni etiche, giuridiche e politiche delle tecnologie digitali	39
Teoria e modelli di governance	41
Responsible Research Innovation (RRI).....	43
Il regolamento generale protezione dati personali/GDPR	45
Gamification	48



Diritto privato: definizione, fonti, soggetti, regolamenti (inizio parte Viglione)

Dove c'è l'uomo c'è diritto; qualunque organizzazione sociale costituisce un ordinamento giuridico, configurato come sistema e possedendo 3 caratteristiche: unitarietà, completezza e coerenza. Si può definire il diritto in un'accezione soggettiva (diritto in senso soggettivo), riconosciuto ad uno o più soggetti di agire per la realizzazione di un interesse oppure anche in senso oggettivo, come una serie di regole che normano la condotta degli individui. Complessivamente il diritto può essere definito come un insieme di regole giuridiche e quindi di norme, regolate da sanzioni nel caso di non adempimento e/o rispetto della stessa.

Una regola giuridica è generale ed è astratta, in quanto è rivolta a tutti i soggetti di una certa comunità. Questo insieme di regole può essere definito prescrittivo, quindi sono dei precetti che esprimono dei comandi, quindi la necessità di comportarsi in un certo modo. Si dice quindi che abbiano un carattere coercitivo. Queste regole sono astratte, quindi appunto a seconda del contesto sono suscettibili di un'applicazione indefinita chiaramente della regola in sé ma definita dal contesto stesso e generali, rivolgendosi non ad un soggetto unico ma ad un insieme di soggetti.

Ecco quindi che consideriamo l'ordinamento giuridico come insieme di regole prodotte in conformità ad un apparato di fonti e per l'organizzazione di un gruppo sociale. Da questo abbiamo anche le fonti, cioè tutti gli atti e i fatti da cui si originano norme giuridiche. Si deve essere posti a conoscenza di una certa norma giuridica e delle sue conseguenze; qui abbiamo le fonti di cognizione, per far conoscere ad una comunità che esistono. Ovviamente non è ammessa la non conoscenza di una certa regola; un cittadino è quindi tenuto a conoscerla e rispettarla. Similmente, abbiamo anche le fonti di produzione, quindi una serie di atti/fatti in cui si originano le norme giuridiche.

Le fonti sono espresse in maniera gerarchica e ciò viene definito dall'articolo 1 del Codice civile, creato nel 1942, in particolare definendo una distinzione netta tra le leggi, regolamenti, norme corporative (leggi che regolano le corporazioni, che esistevano in epoca fascista e non più molto applicabili) e gli usi/consuetudini. Esse vanno interpretate dal giurista, in maniera astratta al di sopra delle leggi, ponendo sopra a tutto la Costituzione, entrata in vigore nel 1948.

Un quadro più completo delle fonti disponibili, partendo dalla Costituzione, il trattato dell'Unione Europea e legislazione comunitaria, la legge (descrivendo leggi parlamentari, decreti legislativi, decreti-legge, Codice civile, ecc.), i regolamenti e gli usi, specificando questi ultimi che si applicano se presenti e devono essere richiamati dalla legge, altrimenti rimangono solo dei gesti o delle abitudini non regolati da norme; i regolamenti invece hanno sempre una legge dietro di sé.

Parlando della Costituzione, essa definita come Fonte sulle fonti, viene definita rigida, cioè modificabile solo attraverso un procedimento più gravoso rispetto alla legislazione ordinaria, oppure rispetto a idee simili come era lo Statuto Albertino, venendo dall'esperienza fascista. Entrambe le Camere devono approvare la legge in una prima delibera con una maggioranza semplice, cioè il 50% + 1 dei votanti, cioè coloro che in quel momento hanno votato; nella seconda delibera, con distanza non inferiore a 3 mesi, deve esserci una maggioranza assoluta, quindi il 50% + 1 degli aventi diritto al voto. Può essere richiesto un referendum popolare se nella seconda votazione la legge non è stata approvata dai due terzi dei componenti delle Camere.

Nel caso di procedimento aggravato, la stessa legge deve essere approvata due volte da entrambe le camere, altrimenti normalmente basta una singola approvazione da parte della Camera e poi del Senato.

La revisione costituzionale pone dei limiti, come stabilito espressamente dall'articolo 139 della Costituzione; quindi, appunto si parla di limiti espressi. Si parla poi di limiti impliciti, quindi dei limiti dati dai diritti fondamentali e questioni da non mettere in discussione, preservando altri diritti costituzionali.

Il rapporto giuridico in gioco è quello tra l'individuo e lo Stato, disciplinando i rapporti del singolo con l'apparato statale, soggetto di diritto pubblico.

La Costituzione disciplina anche l'attività dei soggetti privati, nel campo del diritto privato, intendendo con esso un'ampia definizione del diritto giuridico riguardante almeno una coppia di soggetti privati, parlando per esempio di famiglia, matrimonio, proprietà privata, diritti fondamentali dell'individuo. Similmente a prima, il giusprivatista (definito come esperto di diritto privato) dovrà dare un'interpretazione delle regole esistenti, applicando correttamente il dettato costituzionale. I principi costituzionali sono rilevanti sia come criterio interpretativo per altre norme, quindi usati anche in altri contesti a seconda del caso, oppure come norme di immediata applicazione, per esempio le leggi sui diritti umani.

Fonti importanti anche nel nostro ordinamento sono le fonti di diritto europeo, quindi la serie di trattati costituiti dalla Comunità europea e dalla stessa Unione Europea. Una specifica regola nazionale può essere disapplicata nel caso esista un regolamento europeo; nel caso di una direttiva, la cosa non è simile, in quanto una direttiva non è direttamente applicabile. Dallo stato membro deve essere recepito un certo regolamento, i quali possono essere emanati solo nelle materie previste dai Trattati (es.

Lisbona/Maastricht) e hanno efficacia immediata, prevalendo sulla legge interna. Possono esserci invece le direttive, quindi delle prescrizioni rivolte agli Stati membri contenenti dei principi a cui il legislatore dello stato deve adeguarsi; esse devono essere recepite per poter diventare efficaci).

Una direttiva ha un termine di recepimento quindi; incredibilmente (strano ma vero) l'Italia ha difficoltà a recepire certi regolamenti. La direttiva viene usata come strumento di armonizzazione, raggiungendo uno specifico obiettivo entro un termine fissato, mentre il regolamento ha un obiettivo di uniformità.

Una direttiva può essere self-executing/auto-applicativa; quindi, non necessita di un procedimento di attuazione ed è applicata in senso verticale, quindi nello specifico. Il giudice dovrà quindi applicarla direttamente, eventualmente anche disapplicando una certa normativa già esistente.

Una legge ordinaria nasce da una proposta di legge, da parte anche di un singolo parlamentare o del governo, singoli e organi con potere di iniziativa legislativa. Segue poi una fase di promulgazione della legge a cui consegue la pubblicazione in Gazzetta Ufficiale, come mezzo di cognizione della legge approvata. Successivamente ai 15 giorni di vacatio legis, la legge entra in vigore. C'è un principio di non retroattività per una legge penale approvata, con il principio del favor rei, dove la legge viene interpretata a favore del condannato. Anche le regioni hanno potestà legislativa, potendo promulgare leggi loro stesse e non si pongono in posizioni diverse della gerarchia. In queste si applicherà il criterio della completezza per una legge. La legge statale pone il principio fondamentale della materia, mentre la legge regionale pone i principi specifici di un'applicazione.

All'interno di queste descriviamo i decreti-legge, quindi necessità ed urgenza di una legge; essi durano 60 giorni, entro i quali le Camere devono convertirlo in legge. Essi sono atti aventi forza di legge, quindi aventi lo stesso livello gerarchico di una legge emessa dal Parlamento.

Concludiamo descrivendo anche il decreto legislativo, in cui il Parlamento può delegare la funzione legislativa al Governo, a patto che siano determinati nella legge delega i principi e criteri direttivi di un certo decreto.

Decreti, applicazione norme, interpretazione, risoluzione conflitti

Si parla di atti aventi forza di legge, quindi degli atti con più facile emanazione rispetto alle leggi ordinarie e sono emanati dal governo, in casi di necessità ed urgenza.

Come accennato prima abbiamo i decreti-legge ed i decreti legislativi. Se non convertiti, i decreti-legge cadono (cosa abbastanza infrequente, se non che non succede mai). Essi infatti coprono situazioni di emergenza. Il decreto legislativo invece viene emanato dal Governo su delega del Parlamento.

Il conflitto sugli ordinamenti viene risolto in vari modi, per esempio in senso cronologico, quindi la successione di fonti nel tempo, abrogando la fonte più vecchia, gerarchico, regolando i rapporti tra fonti di diverso rango (quindi prevale la legge più forte, per esempio la Costituzione su una legge ordinaria) e anche in competenza, regolando i rapporti sulla base dei differenti tipi di legge e delle differenti materie di applicazione.

L'applicazione delle norme giuridiche, non destinate a rimanere puramente sulla carta, è generale ed astratta, diventando però poi specificata e concreta. Ad esempio, il Codice civile, legge di tipo costituzionale, oppure anche il diritto di famiglia, per cui matrimonio, divorzio, ecc.

Il legislatore applica le norme in maniera indefinita, rivolte quindi ad una pluralità di soggetti (generali), descrivendo un singolo caso, sussunti (quindi concretizzati). In questo caso è il giudice che trasforma un particolare comando risolvendo una controversia attraverso la sentenza.

Esse fungono da criteri di comportamento, quindi una sorta di prescrizione oppure di definizione, dando un chiarimento oppure una disposizione normativa delle leggi. Ad ogni modo il percorso stesso delle norme non è ben definito, in quanto molto spesso nuove regole sono create dalla giurisprudenza, razionalizzate dalla dottrina e poi riconosciute come legge in un secondo momento.

Riconosciamo quindi la legislazione, quindi l'insieme delle fonti, la giurisprudenza, quindi l'insieme delle decisioni dei giudici, ciascuno con una sua competenza e la dottrina, quindi la letteratura specialistica applicabile in determinati casi. La risoluzione dei singoli conflitti spetta a vari organi: per esempio nella risoluzione dei contratti rimasti inadempiti si va in Tribunale. Esistono altri modi di risoluzione dei conflitti nei gradi di giudizio, giudice di pace (per controversie fino a 5200 euro), Corte d'Appello (se il primo grado si è svolto in tribunale, altrimenti se svoltosi innanzi al giudice di pace, allora in secondo grado ci sta il tribunale) e Cassazione (quest'ultima dà le linee interpretative prevalenti, in senso monofilattico).

Altri esempi ancora sono la Corte costituzionale, decidendo se una possibile legge sia legittima o meno da un punto di vista Costituzionale e risolvendo conflitti tra i poteri dello stato. Esempi rilevanti in questo senso sono anche la Corte di Giustizia dell'Unione Europea, interpretando le singole direttive e regolamenti emessi dalle UE oppure anche la Corte Europea dei diritti dell'uomo, atta alla risoluzione di controversie riguardanti questioni "di un certo peso" (es. diritto alla riservatezza, diritto alla vita, non discriminazione, ecc.)

Altra cosa importante è l'interpretazione, quindi l'attribuzione di un significato delle parole o dei contenuti dati dal legislatore, stabilendo ad esempio quale, tra le norme possibili, sia la regola che si addice al caso che si ha dinanzi, attribuendole un corretto significato. Tutte le procedure normative richiedono questo procedimento. Esempio semplice è l'imbiancatura di una stanza, per ambiguità del linguaggio magari vengono segnati più metri quadri nel prezzo finale, perché non stabilito nel contratto a monte.

L'interpretazione della legge viene realizzata anche per mezzo di precedenti, nel caso ad esempio di leggi penali. Secondo l'articolo 12 del Codice civile, "Nell'applicare la legge non si può ad essa attribuire altro significato che quello fatto palese dal significato proprio delle parole, secondo la connessione di esse, e dalla intenzione del legislatore", cercando di capire l'effettiva interpretazione, in senso finalistico.

Un esempio interessante è lo scarso numero di articoli in ambito di responsabilità civile. Il contenzioso che deriva da questi è molto ampio e il loro processo interpretativo è molto cambiato nel corso del tempo, adattando meno norme a numerosi contesti.

Un caso utile di risoluzione dei contenziosi è dato da incidenti stradali, provocando volutamente oppure accidentalmente; in entrambi i casi se ad esempio ferissi un individuo ad una gamba, il prezzo da pagare rimarrebbe comunque lo stesso.

Il legislatore potrebbe non aver previsto una particolare fattispecie interpretativa di una situazione fonte di controversie ed il giudice non può rifiutarsi di dare giustizia; tale principio è regolato da strumenti di integrazione del diritto, cercando di colmare lacune/vuoti normativi (principio di completezza).

Questo è il procedimento di analogia, vedendo se mancano regole disciplinanti casi simili (*analogia legis*) oppure tramite la lettura dei principi generali dell'ordinamento giuridico (*analogia iuris*).

Concludiamo citando l'articolo 12, "Se una controversia non può essere decisa con una precisa disposizione, si ha riguardo alle disposizioni che regolano casi simili o materie analoghe; se il caso rimane ancora dubbio, si decide secondo i principi generali dell'ordinamento giuridico dello Stato".

Contratti digitali: disciplina generale, stipula, terminologie

Qualunque tipo di contratto è disciplinato dal Codice civile, linea guida per regole generali (art. 1321 e successivi, come ad es. 1325). Esistono quindi i contratti tipici/tipizzati dal legislatore, tipo di contratto classico e per cui esiste uno schema espressamente previsto dall'ordinamento giuridico, con disciplina dettata dal Codice civile o da una legge speciale (es. contratti di scambio, reali, bancari, ecc).

Il principio fondamentale è quello della autonomia contrattuale, dando libertà di autodeterminazione della natura del contratto e della controparte contrattuale, scegliendo anche un tipo di contratto atipico (non tipizzato dal legislatore, poiché solo regolato dalle due parti sulla base del principio appena enunciato).

Nel caso della stipulazione di un contratto, una volta pagato il prezzo, alla conclusione del contratto si cristallizzano gli effetti del rapporto giuridico, non avendo quindi diritto di restituzione. La cosa cambia in un caso specifico, cioè quando il contratto è concluso *a distanza*.

Si ha quindi il *principio di buona fede*, quindi il "fidarsi" banalmente che la disciplina del contratto e del rapporto in uso abbia senso.

Esso si basa su un accordo, fondendo le volontà delle parti in oggetto. Una proposta deve essere assolutamente identica all'accettazione del contratto seguendo la *mirror image rule*. Nella fase di contrattazione devo essere onesto, pena risarcimento danni. Non si è obbligati alla stipulazione di un contratto, tuttavia in fasi avanzate o ad accettazione delle conclusioni dello stesso viene considerato accettato e non si ha la possibilità di contestarlo (pena risarcimento per slealtà nell'accordo).

Deve sempre esserci una causa nel contratto, dunque una funzione economica e tale che abbia un certo significato, solitamente di natura economica. Naturalmente la stipulazione di un contratto può essere o meno lecita, in particolar modo su un'operazione economica e giuridicamente deve essere, nei limiti del rapporto contrattuale, possibile portarla a termine. Naturalmente un contratto deve avere chiaramente indicato un oggetto, quindi l'insieme delle prestazioni che le parti si obbligano a fornire reciprocamente.

Esso deve essere *possibile* (attuabile concretamente a seconda del contesto, ad esempio un privato non potrà vendere un bene del Demanio), *lecito* (affinché non violi norme esistenti) e *determinato/determinabile*, individuato e ben conosciuto da entrambe le parti (ad esempio, contratti di borsa, caso *determinabile* perché il valore varia a seconda del tempo, oppure il contratto di un immobile, caso *determinato*).

Altro requisito utile è la forma, esempio è la forma tacita/autoconcludente, dato da "una compravendita dimostrata con fatti concreti e con un contegno che sarebbe incompatibile con una volontà diversa dai fatti" (es. pagamento ad una cassa automatica, non si hanno parti fisiche con cui interagire ma le intenzioni sono chiare e dettate dall'individuo stesso), oppure forma espressa, con una manifestazione esteriore, di molteplici tipi (i.e. tramite un accordo verbale/scritto).

Nella fase di stipulazione dei contratti si considera che alcuni siano solo scritti (ad es. compravendita di beni immobiliari) per trascrivere la registrazione dell'avvenuto accordo, specie se sotto forma di atto pubblico, essendo contratti importanti ed imponendo un vincolo legale/formale severo (in caso ad esempio della nascita di una società) oppure anche tramite le donazioni, parimenti al caso precedente. Per entrambi è necessaria una trascrizione e regolamentazione da parte del notaio, che ne garantisce l'autenticità. Ciò accade anche per i beni di modico valore oppure di valore non ben conosciuto. Un esempio lampante può essere il padre che generosamente dona un'ingente quantità di denaro al proprio figlio; tutto ciò deve avere un senso legalmente, fiscalmente ed ereditariamente, dando la giusta validità all'azione.

La stipula del contratto avviene tramite diverse modalità, ad esempio scambio di e-mail, tale che siano simili le proposte; quando chi ha fatto la proposta viene a conoscenza dell'accettazione, il contratto è concluso. Ad una richiesta via e-mail/web segue l'esecuzione per fatti concludenti con l'inizio dell'esecuzione.

Un'altra forma di stipulazione è quella di offerta al pubblico, per esempio l'acquisto tramite un sito web (facendo clic, tramite click wrap agreement), ponendo dei problemi per il consumatore; in questo caso il click sull'icona è più che sufficiente a determinare la conclusione dell'accordo. In questo specifico ambito, magari in vendite al dettaglio più piccole, si può cercare di raggiungere la vendita tramite trattativa, nel caso in cui i termini di acquisto non siano ben specificati. Ciò non è reato di per sé; ovviamente dipende dal contesto. Inoltre, ad una richiesta (via e-mail o via web) segue l'esecuzione e la terminazione si ha per fatti concludenti con l'inizio dell'esecuzione.

In questo contesto non si ha modo di sapere per certo *chi c'è dall'altra parte* quando si stipula un contratto o si ha un rapporto giuridico. Questo è particolarmente importante quando si ha anche fare con soggetti di età minore ai 18 anni, i quali non hanno capacità giuridica di *agire*; diventa evidente il rischio che si pone sia a livello di dati trasmessi che del loro controllo.

- Ad esempio, nella compravendita di un immobile, il minore lo può comprare esclusivamente per mezzo di un tutore/genitore, non compiendo validamente un atto giuridico volto al proprio interesse. Delle eccezioni a questo fatto sono gli *atti di vita quotidiana* (per esempio, fare la spesa, piccoli acquisti fisici/online, ecc.). Possono essere annullati dei contratti firmati da un minore, costringendo magari l'annullamento di un acquisto.

Nel caso "spinoso" dell'iscrizione ai social network, pur avendo ciascuno un suo regolamento di iscrizione in termini di età e di tempi, si considera che debbano comunque rispettare le norme già esistenti in un paese (ad esempio facendo in modo che siano solo persone maggiorenni a potersi iscrivere, nonostante sia detto diversamente dal regolamento di un sito o di una applicazione).

Prendiamo il caso dell'Italia dove il regolamento sui dati personali è lecito solo a partire dai 16 anni ma l'Italia lo considera lecito solo dai 14. Anche qui, similmente ad altri casi, tutto dipende esclusivamente dal tipo di contesto di applicazione. In generale, alcuni contratti richiedono la forma scritta (art. 1350), quali:

- Contratti che trasferiscono la proprietà di immobili
- Contratti che costituiscono, modificano o trasferiscono il diritto di usufrutto su beni immobili
- Contratti che costituiscono la comunione su beni immobili
- Contratti di locazione di beni immobili per una durata superiore a nove anni
- Contratti di società e di associazione

Per tutti questi occorrerà *una firma elettronica semplice o avanzata*.

Contratti digitali: clausole/reso/diritti vari

Nei contratti, ciascuna causa/effetto dei singoli contratti deve essere stabilita e concordata tra le parti, in particolare tutto deve essere approvato per iscritto. Le condizioni generali di contratto predisposte da uno dei contraenti sono efficaci nei confronti dell'altro se al momento della conclusione del contratto questi le ha conosciute o avrebbe dovuto conoscerle usando l'ordinaria diligenza.

Già il Codice civile prevedeva una prima forma di protezione per i contratti standard; qui la controparte può solo prendere/lasciare il contenuto di un contratto, in merito alle clausole, dichiarandole riconoscibili per la parte aderente, comportandosi in maniera corretta. Per renderle riconoscibili le regole/clausole devono essere note a priori; in ogni caso *non hanno effetto, se non sono specificatamente approvate per iscritto*, le condizioni che stabiliscono, a favore di colui che le ha predisposte:

- Limitazioni della responsabilità
- Facoltà di recedere dal contratto
- Decadenze
- Limitazioni alla facoltà di opporre eccezioni
- Restrizioni della libertà contrattuale nei confronti di terzi
- Tacita proroga o rinnovazione del contratto
- Clausole compromissorie

Un'altra categoria sono le clausole vessatorie, a vantaggio solo di una delle due parti. Il legislatore impone una particolare attenzione, per ponderarle e capirle, in quanto danneggiano diritti ed obblighi del consumatore. Ad esempio, una delle due parti può esprimere la propria mancanza di colpa/responsabilità, viene ritenuta valida, ma deve essere chiara da subito. Stessa cosa anche la recessione del contratto, ma anche le generali decadenze.

Qui l'Autorità può accertare la vessatorietà della clausole attivandosi o pronunciandosi se interpellata a favore del consumatore, in quanto normalmente si tratta di svantaggio per il firmatario (normalmente firmate almeno due volte), tali che una delle due parti non paghi nulla nella recessione da un accordo rispetto all'altra. Si notano orientamenti difformi in giurisprudenza (per esempio, nel caso del sistema *point and click*). Sembra preferibile quello positivo (es.: Trib. Napoli 2018), altrimenti tutti questi contratti sarebbero vincolati alla firma digitale (e alla forma scritta, non prevista dalla legge).

Ulteriore categoria sono le clausole compromissorie, dove le parti rinunciano al tribunale e accettano di prendere giustizia da parte di arbitri (giudizio esterno). La clausola delega la normale competenza di un tribunale, esprimendo esplicitamente per iscritto questa regola ed è una clausola indipendente.

La stessa cosa deve essere nota anche in ambito digitale, nell'ambito *point and click* di adesione, in maniera tale che sia chiaro che l'attenzione del cliente è richiesta per specifiche clausole vessatorie, dando loro approvazione. Il diritto si adatta e riconosce che il sistema sia rispettato da un punto di vista legale, piuttosto che apporre una firma digitale ad ogni singola forma di accordo.

Negli stessi abbonamenti sono anche diffuse determinate clausole di rinnovamento del contratto, cambiando in meglio o in peggio; in questi casi, deve essere ben disponibile la rescissione del contratto. Più in generale vi sono orientamenti difformi in giurisprudenza, preferendo un orientamento positivo.

Le clausole abusive comunque entrano a far parte dei contratti, rivelandosi comunque inefficaci, ad esempio la clausola del dolo o non rispondendo della morte del consumatore. Di fatto si impedisce al contraente di contrattare le clausole abusive; problema tuttora che rimane aperto, quindi un contratto dove si pone modifica del contenuto da parte del cliente.

Possono essere messi in discussione i contratti o le clausole, come fa spesso AGCM, citando il “Codice del Consumo” che contiene la regolazione in merito alle clausole abusive, valutando il contenuto di queste. Le controversie possono essere risolte in maniera extragiudiziale, adicendo organi extragiudiziali anche per via telematica (es. Facebook, con un proprio sistema giudiziale di approvazione dei contenuti).

Le fonti in materia: Direttiva 93/13/CEE - Direttiva 2019/2161/UE - Codice del consumo, art. 33 (lista grigia e lista nera di clausole abusive).

- Esempio importante: WhatsApp. È stato certificato da una sentenza che la responsabilità di mantenimento e funzionamento dell’applicazione è completamente in mano al cliente; importante nel caso di lucro cessante, quindi il fatto che uno non possa guadagnare a causa di problematiche particolari (mancato guadagno o danno emergente per perdita subita). In caso di controversia, determinate clausole possono non entrare a far parte di un contratto.
- Altro esempio: gli influencer, che pubblicizzano un prodotto magari non dicendo di essere pagati. Il consumatore deve essere reso partecipe dell’accordo pubblicitario. In tutte queste situazioni, l’authority garante interviene (di tanti tipi, AGCM regola la concorrenza, il garante della privacy, ecc.).

Il decreto legislativo 70/03 in materia di commercio elettronico stabilisce il divieto di autorizzazione preventiva di esercizio delle attività, quindi senza approvazione nell’apertura di un commercio elettronico, specie in siti di e-commerce (B2B, business-to-business, B2C, business to consumer).

Stabilisce quindi l’obbligo di *informazione*, dando all’utente tutte le informazioni possibili, banalmente perché sto vendendo un bene a distanza, indicando tutte le caratteristiche di un servizio.

Tutte queste caratteristiche sono regolate dall’articolo 49/Codice del consumo delineando:

- le principali caratteristiche e proprietà di un certo servizio
- l’identità del professionista, l’indirizzo di riferimento, le modalità pagamento e consegna (modalità/tempi),
- diritto di recesso (*ad nutum/secondo la volontà*), reso (entro 14 giorni dalla conclusione), diversa disciplina nel caso di malfunzionamento/danno (ad es. la garanzia, che c’è sempre anche se non esplicitamente presente).
- *garanzie*, situazioni a vantaggio del consumatore nel caso di malfunzionamento/difetti di un prodotto, previste per il consumatore entro un certo periodo di tempo. Anche nel caso di danni è possibile chiedere la riduzione del prezzo, scegliendo lo stesso il prodotto. Similmente vi è anche la sostituzione del prodotto stesso, restituzione, risarcimento e vari provvedimenti su questa linea.

Ovviamente tutto ciò deve essere rivolto al venditore e non al produttore.

Nel caso di un particolare danno provocato da un prodotto molto difettoso (che causa danni grossi) risponde il produttore (esempio che pongo io, telefoni Samsung qualche anno fa noti per esplodere improvvisamente o anche il malfunzionamento di una protesi medica, causando un ulteriore danno oltre a quello già presente). In quanto consumatore, egli deve possedere la possibilità di fare causa liberamente al produttore/venditore. Nel caso di recesso, se il consumatore non viene messo al corrente della possibilità di rescissione, il periodo di reso si allunga moltissimo a beneficio del cliente; assieme alle garanzie, il reso è il più importante.

In caso di controversie, prestatore e destinatario del servizio della società dell’informazione possono adire anche organi di composizione extragiudiziale che operano anche per via telematica (*composizione extragiudiziale delle controversie*).

Il codice del consumo si applica nei *contratti a distanza* tra professionista/fornitore e consumatore.

Non viene sempre applicato, per esempio:

- nei servizi finanziari, dato che essi hanno normative specifiche a loro dedicate
- contratti tramite distributori automatici/locali automatizzati (autoconcludenti)
- contratti conclusi in vendita all'asta
- contratti relativi alla costruzione/vendita di beni immobili (escludendo la locazione)
- contratti conclusi con operatori delle telecomunicazioni con telefoni pubblici

Come preannunciato, il diritto di recesso (artt. 52-59 cod. cons.) si ha entro i 14 giorni lavorativi:

- nel caso di beni, dal giorno del loro ricevimento
- nel caso di servizi, dal giorno di conclusione del contratto. Nel caso di non informazione, si ha entro tre mesi.

Anche qui non si esercita in vari casi (la maggior parte casi di buon senso):

- generi alimentari, per ovvi motivi dati diciamo dalla deperibilità/deterioramento del bene
- servizi di alloggio/trasporto/ristorazione, fornendo prestazioni in una certa data/periodo
- beni/servizi in cui il prezzo fluttua a causa di tassi del mercato
- beni confezionati su misura e deteriorabili
- prodotti audiovisivi/software informatici sigillati, se aperti dal consumatore (ormai antica questa come immaginabile)
- fornitura di giornali

Già dal caso napoleonico, si pensa il contratto come una legge, non avendo una rescissione unilaterale, a meno che (come effettivamente è), non sia stabilito dalla legge la possibilità di rescinderlo.

Esistono deroghe a contratti stabili, es. i contratti di lavoro, in cui il capo può in alcuni casi licenziare il cliente o contratti di locazione, dando un certo periodo di preavviso (normalmente sei mesi).

Il fornitore ha alcuni obblighi:

- Deve dare adeguate informazioni al consumatore
- Deve dare conferma scritta delle informazioni
- Deve permettere l'esercizio del diritto di recesso
- Deve eseguire l'ordinazione entro 30 giorni salvo diverso accordo

I diritti attribuiti al consumatore sono irrinunciabili, dando adeguate informazioni e dovendo avere conferma scritta delle stesse, fornendo l'esercizio del diritto di recesso.

Anche sotto forma di clausole vessatorie firmate, il consumatore ha sempre diritto di tutela.

Altro caso importante è la *tutela del minore*, perché non ha giuridicamente la piena capacità di comprensione/agire, assumendo una linea di comunicazione chiara in quanto sono soggetti *particolarmente vulnerabili* (codice consumo art. 52) e il fatto che i servizi dello stato sono limitati, tutelando il giusto i minori, proteggendoli (decr. leg. 70/03, art.5/18).

Bisogna infine definire un sistema di tutele per chi usa servizi/motori di ricerca online, redando i termini d'uso, limitando e cessando gli account in particolari caso e garantendo che le offerte per il sito web ed il sito stesso, affinché si abbia una corretta limitazione di tutte queste pratiche.

Contratti digitali: controversie e smart contracts. Diritto dei beni: introduzione

Nelle controversie si cerca di conciliare le parti. Le controversie sono di natura commerciale (relative a beni/servizi, pagamenti, violazioni di diritti) oppure di natura non commerciale (violazioni di privacy, diffusione di contenuti diffamatori/offensivi/spam).

Naturalmente le controversie possono essere dispendiose sia a livello di tempo che a livello di costi, crescendo le singole dispute di valore economico/commerciale anche scarso fino a quelle di livello internazionale, tutte con tempi lunghi ed incerti.

Molte di queste fanno parte di un insieme di casi per cui esiste un insieme specifico di tutele: ad esempio, secondo il regolamento UE 1150/2019, viene definito un sistema di tutele per i professionisti dell'intermediazione online e per i motori di ricerca. In particolare, si fa riferimento alla redazione dei termini d'uso, limitazione/sospensione/cessazione degli account e posizionamento di offerta/sito web.

Nel caso di B2B/B2C si hanno generalmente controversie:

- relative ai beni e servizi oggetto della transazione;
- relative ai pagamenti;
- relative a violazioni di diritti (diritto d'autore, nome a dominio).

Nel caso invece di controversie di natura non commerciale se ne hanno:

- relative a violazioni della privacy;
- relative alla diffusione di contenuti diffamatori o offensivi;
- relative allo spamming.

In merito all'*ADR (Alternative Dispute Resolution)* online, nel caso di giudizio esterno, vi è l'arbitrato online; in questo caso ha "diritto di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato" (art 22 reg. 679/2019 UE), quindi non si può pensare che l'utente sia sottoposto a questo tipo di decisione (es. WIPO Arbitration Center). Similmente si ha la mediazione online, con accordo finale tra le parti tramite negoziazione prevalentemente in rete; essa si prefigura come alternativa.

Nel 2013 la stessa UE ha reso disponibile una piattaforma di ORD (Online Dispute Resolution) tramite cui attivare la procedura stragiudiziale di risoluzione delle controversie relative all'acquisto online di prodotti o servizi (es. Amazon che ha espressamente richiesto questa modalità); si intende che l'accesso alla giustizia ordinaria non viene, comunque, precluso in alcun modo.

Un tipo di contratto automatico, tradotto come codice informatico senza manifestazione di volontà, sono gli smart contracts. In questi casi le problematiche sorgono: per esempio, cosa succede nel caso di un malfunzionamento di un software, chi è responsabile? Le regole del diritto cercano di regolare il fenomeno. È possibile revocare il proprio consenso in base al tipo di impegno iniziale; di fatto questo è abbastanza discutibile. Questo tipo di contratto è totalmente automatico e viene usato soprattutto nella blockchain. Una volta stipulato un accordo, verificato, bloccando chi non può accedere, in automatico permette accettazione/rifiuto di transazioni, ragionando come un "if-then-else".

Parliamo ora di beni, le regole sono nel terzo libro del Codice civile, che ha subito meno modifiche di tutti gli altri pezzi. La principale divisione è tra beni immobili (beni normalmente/artificialmente incorporati al suolo) e beni mobili (tutto ciò che non è immobile). Alcuni beni hanno regole intermedie tra le due, i cosiddetti beni mobili registrati (es. navi/aerei/auto, quindi mezzi che circolano).

I contratti che hanno ad oggetto i beni mobili possono svolgersi interamente online; in generale tra questi cambia il "regime di circolazione", quindi la regolamentazione specifica e la pubblicità.

Non per forza deve essere un bene materiale, per esempio beni immateriali (risorse intangibili e incorporali); non dobbiamo quindi essere tratti in inganno, dato che qualunque tipo di diritto può essere

oggetto di regolazione. Tra questi rientrano anche opere dell'ingegno, invenzioni industriali, segni distintivi di un'impresa (quello che caratterizza un'azienda, un marchio, e anche questo rappresenta un bene), diritti audiovisivi o anche immagini del bene stesso (d. lgs. 10/02/2005).

Similmente anche un *software*, definito come supporto logico/informatico che risolve un certo problema, composto da un insieme specifico di istruzioni interpretato da un elaboratore e può essere compravenduto. Anch'esso rientra nella definizione di bene, ad esempio anche nel caso di una licenza.

Tutte queste regole sono disciplinate da un decreto legislativo del 2005; dalle varie regole del software vi sono la pubblicazione, riproduzione, modificazione, comunicazione al pubblico e pubblicazione in raccolta (in maniera esclusiva); da questi restano esclusi uso/correzione di errori, copia di backup, studio del funzionamento, nonché interoperabilità.

Il diritto di *proprietà* aderisce al modello di mercato occidentale, dando alla proprietà una funzione sociale. La sua definizione è "il diritto di godere/disporre della proprietà in modo esclusivo, entro i limiti e obblighi dell'ordinamento giuridico, godendone a proprio vantaggio".

Posso similmente escludere altri dal godimento di un bene e alla disposizione dello stesso.

Nell'uso di un bene, limite fondamentale è il non recare danno ad altre persone/beni (divieto di atti emulativi, ad esempio il bruciare le sterpaglie, alberi alti, palizzate nei confronti del vicino per dare fastidio o scopi illeciti). Altre domande più teoriche si pongono in merito a beni artistici (se consentirne o meno il libero utilizzo o la distruzione; ciò è astratto e dipende dal contesto).

Altro diritto regolato dal Codice civile è il *possesso*, regolato dall'articolo 1140 del Codice civile. Esso è il potere sulla cosa che si manifesta in un'attività corrispondente all'esercizio della proprietà. Il *possessore* è colui che si comporta come fosse il proprietario; se non lo è, l'ordinamento non è indifferente.

Nel caso di una controversia in cui si compra un bene da una persona che lo ha rubato e per qualche motivo il proprietario originario la ritrova, comunque la proprietà è acquistata dal nuovo possessore, grazie alla consegna e all'acquisto, purché sia in buona fede.

Similmente si ha il concetto di *usucapione*, che a causa del lungo periodo di possesso indisturbato del bene diventa a tutti gli effetti il proprietario. Ovviamente non si può modificare la detenzione in possesso con la sola volontà (es. l'inquilino che pretende smettere di pagare un canone di affitto e pretende di diventarne proprietario).

In merito invece alla *proprietà industriale*, esiste un apposito codice regolatore (Codice della proprietà industriale/C.p.i) i cui diritti si acquistano mediante *brevettazione* (vale 20 anni), *registrazione* o altri modi previsti, dando luogo ai *titoli di proprietà industriale* è un mondo complesso.

- Sono oggetto di brevettazione sono invenzioni, modelli di utilità, nuove varietà digitale.
- Sono oggetto di registrazione sono i marchi, disegni/modelli, topografie di prodotti a semiconduttori.

In merito all'uso anche di un marchio, se l'uso è brevettato/registrato prima è utilizzabile anche se io stesso lo possedevo. La stessa proprietà industriale non riguarda i siti internet, per cui è possibile usare un prodotto con il nome del sito, ma non il sito stesso.

Più in generale essa riguarda principalmente lo sfruttamento economico della stessa proprietà dimostrata.

Non si devono violare le *privative*, quindi un insieme di diritti esclusivi, riconosciute per tutelare lo sforzo creativo di un oggetto, trattandosi quindi di diritti di carattere patrimoniale.

Al creatore è anche riconosciuto il "*diritto morale alla paternità dell'opera*", che ha una specifica durata prestabilita per legge, con un diritto morale di possesso che deve sempre essere riconosciuto.

Nel caso di opere letterarie, viene riconosciuta una privativa di 70 anni.

Parliamo poi di *tutela del software*, disciplinata dal Codice civile nell'articolo 2575 facendole rientrare nella generica definizione data dallo stesso, cioè «*formano oggetto del diritto di autore le opere dell'ingegno di carattere creativo che appartengono alle scienze, alla letteratura, alla musica, alle arti figurative, all'architettura, al teatro e alla cinematografia, qualunque ne sia il modo o la forma di espressione*», con un diritto morale non cedibile ma sempre trasmissibile agli eredi.

Il fatto stesso della creazione fa sorgere il diritto d'autore (altri riferimenti, Legge 633/1941 (Legge sul diritto d'autore) e D.lgs. 518/1992, in attuazione della Direttiva 91/250/CEE).

Diritto d'autore, Successione nel patrimonio digitale

L'interrogativo principale, quindi, è porre il diritto di brevettazione per il possesso del diritto d'autore, ottenendolo possibilmente tramite una privativa. Nel caso dei software, appunto, sono equiparabili proprio a dei beni fisici, ma soltanto alcuni programmi possono essere effettivamente brevettati, dando per esempio una particolare funzione tecnica non prima presente sul mercato (es. ottimizzazione PC, gestionali, ecc.). Dura normalmente 20 anni e si segue il principio della protezione della legge sul diritto d'autore, bloccando tutto ciò che risulta identico alla creazione realizzata. In altri casi è consentita la riproduzione, modificazione, distribuzione.

Ciò si realizza tramite il *brevetto*, quindi, dà il diritto di commercializzazione e produzione esclusiva all'interno di un certo Paese o un insieme di Stati per cui è stato richiesto, distinguendo tra:

- 1) *l'invenzione industriale*, soluzione nuova ed originale ad un problema tecnico mai risolto prima
- 2) *il modello di utilità*, oggetti nuovi o modifiche di oggetti già esistenti per renderne più facile l'utilizzo.

Per poter chiedere un brevetto, l'invenzione non deve essere una cosa preesistente (*novità*), risultando nuova ed originale (*originalità*) (ritenuta quindi non compresa nello stato della tecnica accessibile al pubblico e non ritenuta evidente da persone esperte nel ramo), affinché risulti pienamente ammissibile dal punto di vista giuridico, argomentandone la validità (*liceità*) ed utile in ambito produttivo (*industrialità*).

Il secondo principio è quello dell'*esaurimento del diritto di distribuzione*, secondo il quale la prima pubblicazione di un'opera determina l'esaurimento della privativa concessa all'autore. L'opera circola, senza impedire una successiva circolazione del supporto materiale su cui è incorporato il bene, non avendo naturalmente diritto di riproduzione personale (nel caso dei software, essendo magari su supporto elettronico, si seguono le regole ordinarie dei beni mobili).

Lo sviluppatore di un software è titolare di diritti esclusivi sul *codice sorgente* e sul *codice oggetto*, sapendo che il primo è *l'oggetto puro di creazione, interpretato* e quindi creato sotto forma del secondo da un *insieme di macchine e dispositivi*. La creazione di un nuovo programma a partire da quello già esistente è impossibile in assenza del trasferimento del diritto d'autore.

Deve essere riconosciuto il diritto d'autore da parte del primo creatore del software, permettendo la giusta riproducibilità solo in caso di esplicito permesso, ottenuto dietro pagamento di corrispettivo.

Nel caso dei software, naturalmente, questa è la situazione del tipo *closed source*, rispetto invece agli *open source*, liberamente modificabili (dipende anche lì, magari ci sta una licenza "a metà" come la Creative Commons). Diverso è il modello dell'*open software* (le licenze open source concedono in uso il software nello stato in cui si trova, non garantiscono l'assenza di difetti, gli utilizzatori possono modificare i codici). Di fatto, concludendo, un'opera viene considerata originale solamente se possiede un "*significato poetico e letterario distinto, con un certo scarto semantico*", tale da distinguere il perché una certa cosa sia nuova ed effettivamente creativa.

Si cerca quindi, da un punto di vista europeo di Direttiva (*direttiva sui contenuti digitali 2019/770/UE*), di equiparare la posizione del consumatore di beni digitali a quella dei beni “tradizionali”, venendo riconosciuto il diritto di ripristino del contenuto in caso di difetto di conformità o a una riduzione adeguata del prezzo/risoluzione del contratto sulla base delle condizioni stabilite dallo stesso in merito all’articolo in oggetto. Si applica a qualsiasi contratto in cui l’operatore economico fornisce contenuti o servizi digitali al consumatore e il consumatore corrisponde un prezzo. L’onerosità del contratto diventa quindi un requisito essenziale affinché il consumatore possa godere dei diritti introdotti dalla direttiva.

Lo stesso operatore economico assicura al consumatore la notifica/conoscibilità delle proprie condizioni di servizio/contratto, fornendo aggiornamenti, anche di sicurezza, necessari a mantenere la conformità del contenuto/servizio digitale. Se il consumatore non installa determinati aggiornamenti (articolo 8), è ritenuto responsabile di possibili difetti di conformità al prodotto; l’articolo 14 della direttiva cita infatti: *“In caso di difetto di conformità, il consumatore ha diritto al ripristino della conformità del contenuto digitale o del servizio digitale, o a una riduzione adeguata del prezzo, o alla risoluzione del contratto sulla base delle condizioni stabilite nel presente articolo [...]”*

Parliamo poi dell’eredità nel mondo digitale di *successione*, ambito dove nascono spesso conflitti e nelle sue modalità di utilizzo (social media, account, tutta una serie di beni immateriali ma che assumono un significato anche economico ma privato, definendo l’identità digitale dell’utente).

Si discute inoltre come, in sé, il *“patrimonio digitale”* rappresenti l’insieme di dati/informazioni riferibili ad una persona e che questa affida al web nelle singole modalità di utilizzo (password, account, cloud, chat), stabilendo per ognuno di essi diritti di accesso e responsabilità connesse alla possibile perdita, regolandone a questo punto eventualmente la successione. Tali dati, a meno che non diversamente specificato, sono imperituri, quindi rimangono presenti per molto tempo. Normalmente il possesso di tutti i dati digitali finisce agli eredi, ma appunto ne si può impostare specificamente l’assegnazione (es. Facebook con l’opzione “Associa l’erede al tuo account”), o rifiutarne esplicitamente il consenso.

Nel caso di alcuni siti, vi possono essere delle clausole inserite per negare la successione agli eredi, talvolta con previsione di distruzione di questi; non basta considerare il contratto, vi è anche un problema di tutela postuma dei diritti della personalità e dei dati personali.

In questo si deve pieno pari diritto, come ai beni fisici, nel caso di discussione tra gli eredi; si instaura infatti una sorta di “comunione ereditaria”. Di fatto nel contratto tra utente e social network, normalmente, si ha la previsione di distruzione di questi contenuti digitali distrutti al momento della morte. Non basta considerare unicamente questo, ma anche il problema di tutela postuma dei diritti della personalità e dei dati personali.

Il testamento *olografo* ha un certo numero di requisiti, tra cui una quota dedicata ai suoi eredi; in particolare, non sarebbe possibile dare tutti i propri beni a un ente esterno rispetto ai soggetti più vicini (quota di riserva). L’Italia accentua particolarmente l’impostazione della famiglia creata formalmente sulla base del matrimonio, non esistendo altri ordinamenti che affermano una cosa simile; ciò conta soprattutto in questo caso, valorizzando la volontà del soggetto preponderante legalmente parlando in merito alla successione.

Diverso è se debba considerarsi giuridicamente tutelato l’interesse altrui, ovvero sia di terzi qualificati (eredi o semplici congiunti), e che siano conservati o disvelati i tratti della personalità del defunto risultanti dalle informazioni raccolte nel web (foto, post, ecc.).

In questo senso, si cita la decisione della Corte Suprema tedesca nel 2018 riguardante una ragazza suicidatasi nel 2012. I genitori non hanno avuto da Facebook l'accesso alla consultazione del profilo e dei messaggi correlati, possibilmente utili a capire se la ragazza potesse aver sofferto di depressione o semplicemente capendo possibili intenzioni. Facebook rifiutava di far accedere i genitori, dato che le condizioni generali del contratto impedivano l'accesso al profilo commemorativo e la lettura dei messaggi. Rimane dibattibile l'utilizzo di questi dati, se considerabile violazione di privacy o se trattati come bene ordinario al momento della successione, assegnando primariamente i beni digitali descritti nella quota di riserva e poi altri eredi, con certificazione da parte del legislatore e autorizzazione del notaio.

Responsabilità civile

Chiunque sia colpevole di provocare un danno, è obbligato a risarcire il danno, per esempio a seguito di un fatto illecito (art. 2043 Codice civile). Si pone l'idea del danno ingiusto (può essere giusto nel caso non contrasti un ordinamento giuridico, ad esempio durante un'operazione medica importante, ad esempio una amputazione, giustificato dall'utilità), ponendosi in contrasto con l'ordinamento giuridico, tramite un nesso di *causalità, colpevolezza (dolo/colpa), imputabilità* (capacità di intendere/volere) e il contesto del danno *ingiusto*. Naturalmente distinguiamo:

- danni provocati a cui consegue un risarcimento (resp. civile, con funzione *compensatoria*);
- danni che richiedono il non rispetto di norme esistenti e conseguente giudizio (resp. penale).
Ad esempio, nel caso della diffamazione, si ha un danno di immagine/reputazione.

In maniera più generale, solo una serie di danni è risarcibile:

- *danni patrimoniali*, cioè quelli che derivano da un evento che intacca la capacità economico-patrimoniale di un soggetto;
- *danni non patrimoniali* (biologici, morali, esistenziali...);
- *danni emergenti*, che sono la perdita economica che il patrimonio del creditore ha subito per colpa della mancata, inesatta o ritardata prestazione del debitore;
- *lucro cessante*, cioè il guadagno che viene meno al creditore a seguito dell'inadempimento o che la vittima perde a causa dell'illecito.

Di fatto, oltre al tipo di danno, si discute in merito al *nesso di causalità*, dando una conseguenza immediata tra il fatto avvenuto e la cagione di un danno preciso/relativo. Il fatto illecito è disciplinabile per principi, date le mille ipotesi della realtà quotidiana, fissando regole più generali possibile (art. 2043 Codice civile). Sulla base dei presupposti, si capisce come effettivamente agire, specializzando l'applicazione dei principi.

Se un soggetto è incapace di intendere/volere, viene giudicato a seconda dei casi (coloro che non capiscono il significato di ciò che stanno facendo, giudicati penalmente in maniera diversa; per esempio, minorenni, soggetti in stato d'ebbrezza, o in ambito lavorativo, dove il titolare giuridico è sempre il datore di lavoro, in ambito assicurativo, dunque in caso di un danno anche provocato da veicoli, ne risponde l'assicurazione).

Nel mondo web, si discute di responsabilità del *provider*, che funge da intermediario della comunicazione tra gestore ed utente finale e risponde o meno a seconda della ragionevolezza del nesso di causalità, rispondendo in merito *al fatto proprio* (fatti illeciti commessi personalmente) o se commesso dall'utente della rete (*per fatto altrui*); la responsabilità è solidale al provider e al terzo, se non vengono provate le condizioni di esonero.

- Di essi vi sono varie categorie, penalmente rilevanti possiamo citare la *cache provider*, mero accumulatore di contenuti automatico/passivo da *hosting provider*, riconosciuto come attivo e penalmente rilevabile in caso di mancata azione nella responsabilità di eventuali illeciti, *content provider*, dunque fornitore di contenuti di vario tipo, *access provider*, che prevede l'accesso ai servizi di rete Internet.

In merito ad un danno provocato da un certo contenuto diffuso sulla piattaforma del gestore, tutto ciò è un interrogativo ponibile. Naturalmente un provider non è assoggettato ad un obbligo generale di sorveglianza, non volendo che la rete sia totalmente segregata, limitando la libertà nella condivisione ed utilizzo di contenuti. Il provider si attiva nel caso di segnalazione a lui fatta, tenendo sempre ad informare senza indugio l'utente (non ancora previsto di preciso dal nostro ordinamento, come invece capita in altri paesi europei).

Si ritiene quindi civilmente responsabile il provider del contenuto dei servizi, specie se non avvisa l'autorità competente se informato dei contenuti illeciti, agendo prontamente e provvedendo (esempi possibili: cyberbullismo, diffamazione, violazione di copyright). Egli infatti non è sottoposto ad un obbligo generale di sorveglianza ed è civilmente responsabile se non ha agito prontamente.

In generale, il provider è responsabile secondo l'art. 2043 del Codice civile, ma la responsabilità è concretamente di chi ha trasmesso/memorizzato le condizioni di esonero, in forma passiva, tecnica ed automatica. La condizione di esonero, quindi la non responsabilità da parte dell'utente, viene provata nel caso di svolgimento dell'attività di controllo in forma automatica e passiva (quindi nel caso ad esempio della rimozione di contenuti considerati coperti da diritto d'autore per cui solitamente si ha una rimozione automatica).

Quindi, fino a prova contraria, è sempre responsabile il provider ma, se viene riconosciuta una condizione di esonero, ne è parimenti responsabile il soggetto terzo fruitore (direttiva 2000/31/CE – d. lgs. 70/2003). Non ha obblighi generali, ma deve essere responsabile di avvisare le autorità giudiziarie/amministrative nei casi giusti.

Il Caso: RTI vs Facebook

I fatti: viene creato su Facebook un profilo dal titolo “*Valentina Ponzzone nei panni di Kilari è assolutamente ridicola*”. All'interno vengono pubblicati una fotografia della Sig.ra Ponzzone nei panni del personaggio “Kilari” e alcuni collegamenti ipertestuali a sequenze di immagini tratte dalla serie animata, con commenti offensivi nei confronti della Sig.ra Ponzzone, derisa per le caratteristiche fisiche, nonché nei confronti di RTI.

La società RTI invia, da febbraio ad aprile 2010, cinque lettere di diffida a Facebook, che però provvede alla rimozione soltanto nel 2012.

RTI e la Sig.ra Ponzzone chiedono giudizialmente i danni: a) violazione del diritto all'onore, alla reputazione e al decoro; b) violazione dei diritti esclusivi di utilizzazione economica sui contenuti audiovisivi della serie animata Kilari di titolarità di RTI.

Decisione Tribunale di Roma: è stata ritenuta illecita la presenza di collegamenti ipertestuali che conducevano alla visione di due sequenze di immagini tratte dalla serie animata trasmessa da RTI e, in particolare, le immagini relative alla sigla iniziale. La messa in rete di un'opera protetta dal diritto d'autore su un sito Internet diverso da quello autorizzato dal titolare del diritto d'autore deve essere qualificata come illecita messa a disposizione del pubblico. In effetti, i link pubblicati su Facebook conducevano non a materiali pubblicati dalla stessa RTI attraverso la propria piattaforma telematica, bensì a materiale pubblicato attraverso Youtube non autorizzato da RTI.

La conoscenza dell'illiceità dei dati memorizzati fa sorgere, in capo al prestatore di servizi, una **responsabilità risarcitoria** (nei confronti di V.P. € 15.000, nei confronti di RTI € 15.5000, di cui circa 8.000 per lesione del diritto d'autore) + **inibitoria**

Il caso: RTI vs DSA

Decisione Tribunale di Roma (gennaio 2021)

il Tribunale di Roma accoglie le domande di RTI volte ad ottenere tutela dei propri diritti connessi all'esercizio del **diritto d'autore** relativi alle attività di produzione ed emissione televisiva, violati dalla messa a disposizione del pubblico, senza autorizzazione, di numerosi brani audiovisivi tratti dai programmi dell'attrice da parte degli utenti delle piattaforme di *video-sharing* "Veoh" e "Dailymotion". Il Tribunale ha riconosciuto la responsabilità dei gestori delle piattaforme, colpevoli di non aver agito per evitare o porre fine alle attività illecite commesse attraverso i propri sistemi. La responsabilità è stata ritenuta derivare direttamente dalla "natura" dei servizi forniti dai due *provider* e dalla qualificazione di questi come *provider* «attivi».

«Condanna la convenuta a risarcire all'attrice i danni, liquidati in complessivi Euro **22.029.700,00** oltre rivalutazione e interessi legali»

Il caso: Vuitton vs Google

Con le parole «Luis Vuitton» e «copia» o «imitazione», su Google apparivano alcuni siti che vendevano prodotti Vuitton contraffatti.

La Corte di Giustizia UE (nel 2011) dichiara che Google non è un provider «passivo». L'organizzazione dei risultati della ricerca e l'indicizzazione lo rendono provider attivo.

Google è quindi responsabile anche prima che Vuitton gli abbia richiesto l'eliminazione di quei risultati della ricerca che potessero essere lesivi dei propri diritti.

Simile l'esito del caso *L'Oréal vs. Ebay*.

Approfondimento per caso L'Oréal vs eBay: <https://www.medialaws.eu/loreal-vs-ebay-protezione-del-marchio-vs-commercio-elettronico/>

Consideriamo anche il caso delle notizie di Google News:

L'art. 15 impone alle società tecnologiche (es.: Google) di pagare gli editori una remunerazione per mostrare estratti da "pubblicazioni di carattere giornalistico", eccetto che si tratti di "utilizzo di singole parole o di estratti molto brevi di pubblicazioni di carattere giornalistico". Uno dei principali obiettivi della riforma del copyright è tentare di obbligare le grandi imprese tecnologiche a condividere i propri ricavi con editori e giornalisti.

Se il fatto illecito venisse commesso da un soggetto diverso dalla piattaforma online ma venisse offerto al pubblico tramite la stessa piattaforma, è dibattibile la possibilità di inadempimento rispetto al servizio che offre, prescindendo dalle condizioni generali. Esempio: Uber risponde della responsabilità dei danni provocati da un incidente stradale di un proprio conducente? Di fatto è simile a quanto detto prima: il datore di lavoro risponde dell'inadempienza alla legge e dei fatti illeciti connessi ai propri dipendenti.

Si sarebbe tentati di rispondere che l'articolo applicato sia il 2049 del Codice civile:

"I padroni e i committenti sono responsabili per i danni arrecati dal fatto illecito dei loro domestici e commessi nell'esercizio delle incombenze a cui sono adibiti"

In taluni casi, parlando ad esempio del danno provocato da una macchina:

- se controllata da operatore umano, ne risponde l'utilizzatore, quindi colui che ha esercitato una manovra colposa/cagionevole di danni (art. 2043 Codice civile)
- se malfunzionamento della macchina, a seconda dei casi, ne risponde il produttore

Nel caso particolare delle macchine AI senza conducente (self-driving cars), cagionando un danno, chi ne risponde tra produttore, programmatore, danneggiato, utilizzatore o il robot/macchina stessa? Nel livello di automazione, se si verifica un livello di controllo del soggetto, si cerca di capire la responsabilità del produttore, capendo se vi sta o meno un obbligo risarcitorio oppure malfunzionamenti di macchina, applicando il regime di responsabilità per difetto. Tuttora tale questione rappresenta un territorio inesplorato, in quanto non esistono concreti casi di applicazione/presenza di mezzi a totale guida autonoma. In alcuni casi, infatti, hanno dovuto rispondere dei danni gli stessi utilizzatori.

Lavoro e tecnologia (inizio parte Sitzia)

Si cerca di capire come il diritto disciplini il lavoro e i limiti applicati alle normative presenti oggi, fornendo quantomeno regole minime di protezione in merito alla protezione del lavoro e delle persone coinvolte nello stesso, disciplinando in modo giusto anche l'ausilio in esso delle tecnologie.

Di fatto il lavoro dignitoso riguarda le persone, che si impegnano attraverso sviluppo di competenze, ad accompagnare l'evoluzione delle tecnologie, specializzandosi per ogni campo d'applicazione e rendendo più agevole la vita stessa ai singoli. Almeno concettualmente *il lavoro non è una merce, ma ha un valore economico*. Dal punto di vista della concorrenza, il diritto del lavoro limita la possibilità di usare il lavoro stesso per parametri prettamente economici. L'introduzione progressiva di tecnologie ha comunque radicalmente influenzato il mondo del lavoro nuovo, infatti, dagli anni Ottanta in poi, l'evoluzione delle tecnologie e della stessa automazione ha portato, oltre alla citata evoluzione di competenze, alla scomparsa di vecchie professioni.

Si sa infatti che oggi sussiste una concorrenza al ribasso, giocandosi sulle regole che limitano l'utilizzo delle nuove tecnologie, con complessi meccanismi di protezione. Ad esempio: utilizzare le telecamere per controllo dei dipendenti, a meno che di non dimostrare di usare questo come mezzo oggettivo (ragioni di sicurezza), piuttosto che ragione di tipo soggettivo. Le regole ovviamente del lavoro cambiano da paese a paese, creando un problema di tipo sociale e realizzando l'obiettivo. La prestazione di lavoro non deve essere delegata rispetto a dove viene mantenuta in modo prevalente (intensità esecutiva nel luogo di esecuzione).

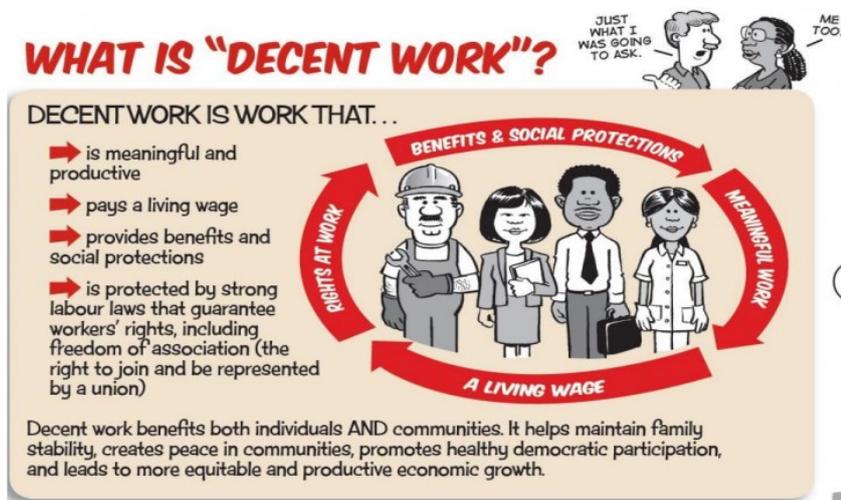
La legge è scelta dalle parti e viene salvata nel luogo di esecuzione della prestazione. Ciascuna deve essere armonizzata, permettendo all'umano di mantenere il controllo sul malfunzionamento della tecnologia. Tutto ciò riguarda in ampia parte la rappresentazione e la protezione stessa del lavoratore, in modo tale che l'innovazione abbia un'ambivalenza di rispetto dell'essere umano spesso utilizzatore e mezzo per la stessa tecnologia (creandosi uno *zoccolo di diritti e protezioni* e che imponga alle piattaforme e ai loro clienti di rispettarle). Lo stesso Rapporto della Commissione Mondiale sull'avvenire del lavoro del 2019 evidenzia questa evidente ambivalenza nel progresso tecnologico, discutendo la qualificazione della relazione di lavoro, la sua durata e la protezione sociale offerta, soprattutto in merito ai diritti collettivi di lavoratori e piattaforme.

La relazione contrattuale è un concetto complicato; nel caso ad esempio della regolamentazione dei rider a chi ci si rivolge, alla piattaforma, l'utente, il ristorante? Quindi fondamentale individuare le parti, tipo di rapporto (di impresa, lavoratore autonomo, subordinato) fornendo una serie di tutele, garanzie e regolamentazioni. C'è un limite all'orario del lavoro o alla durata della prestazione?

Citiamo anche la prestazione sociale e la tutela dagli infortuni, previdenza sociale o diritti collettivi e riunione di sindacati/assemblee. In questi casi la tecnologia in ausilio alla professione è fondamentale sia per regolare il lavoro stesso sia per poter tracciare il dipendente.

L'algoritmo quindi deve stabilire la spartizione di queste informazioni, spartendole alla collettività (partecipazione collettiva), sapendo che c'è anche un problema di informazione (perché la controparte magari non sa quale può essere la logica del programma). Nella loro concezione, le regole del diritto di lavoro devono essere da subito presenti.

Definiamo quindi il *lavoro dignitoso*, soprattutto se mediato da piattaforme digitali, dando il principio del *meaningful* (dando un significato agli obiettivi del lavoratore, anche in senso non produttivo, es. settore terziario), *productive* (garantendo massima produttività con vincoli *strong*, simile alla *strong law*/normativa vincolante, rispetto alla *soft law*, quindi direttive o parametri volontari e responsabilità sociali), la rappresentazione dell'individuo da parte dell'associazione collettiva, con benefici e protezione sociale, nonché uno stipendio a regola delle ore lavorate e commisurato alla professione.



È quindi necessario che i principi che caratterizzano il lavoro dignitoso e le regole base siano già prese in considerazione quando il sistema viene elaborato ed implementato (*decent work by design*, algoritmi e/o sistemi informatici, *approccio fondato sul controllo umano della tecnologia*, come definito dalla OIT-Organizzazione internazionale del lavoro).

Si intende quindi che anche gli algoritmi stessi debbano adeguarsi alle norme professionali esistenti e agli standard presenti, in maniera tale da non uscire dal contesto di applicazione (es. file del Moodle dell'algoritmo di selezione dei docenti; di fatto, essendo algoritmo non ottimamente implementato, i docenti venivano selezionati randomicamente, non più solo sulla base della provenienza ed area geografica, sballando tutto il sistema di scelta).

Necessità di elaborare algoritmi che integrino nella loro concezione il rispetto di un certo numero di standard che caratterizzano il lavoro dignitoso e quindi si abbia un approccio fondato sull'umano al controllo della tecnologia (OIT, Organizzazione Internazionale del Lavoro).

Introduciamo il "*principio dell'autodeterminazione informativa*", circa gli strumenti che elaborano/trattano dati personali e le relative informazioni significative per la logica del contesto utilizzato, specificando il contesto e l'applicazione del controllo a cui i dati della persona sono sottoposti, come spesso avviene nel trattamento automatizzato, avendo il modello europeo che cerca di informare selettivamente e in maniera comprensibile utilizzata, nel caso di un programma (vedi perizia algoritmo selezione docenti).

Il lavoratore ha il diritto di essere *informato* e dispone del libero diritto di *accesso* ai propri dati, in modo *sicuro* e mantenendo tutte le informazioni considerate *significative* (art.13 reg. UE 2016/679, cioè "... *l'esistenza di un processo decisionale automatizzato, compresa la profilazione ... e ... informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato*"). Si cita anche l'articolo 22 del regolamento EU, per cui "*l'interessato ha il diritto di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione, che produca effetti giuridici che lo riguardano o che incida in modo analogo significativamente sulla sua persona*".

Protezione e tutela dell'individuo in ambito reale (fine Decent Work by Design)



A prescindere dalla gestione di terzi, il vero gestore dei dati è sempre il titolare, affidando parimenti ad un soggetto esterno possibili responsabilità. Teoricamente, il titolare attua delle misure per proteggere e fornire un giusto processo di gestione dei dati, sia per protezione che per possibile manutenzione e modifica degli stessi. L'intervento umano si modifica nel corso del processo decisionale e il titolare ha diritto a non vedersi sottoposto a decisioni unicamente automatizzate (art. 22 reg. UE 2016/679).

Da un punto di vista di codice, dunque, l'uso degli algoritmi per valutare le prestazioni dei lavoratori contribuisce alla digitalizzazione della gestione delle risorse umane. Gli algoritmi, infatti, sostituendosi agli esseri umani nella supervisione del lavoro, stanno ridefinendo i rapporti di lavoro.

Rapporto mondiale OIL 2021: https://www.ilo.org/wcmsp5/groups/public/--europe/--ro-geneva/--ilo-rome/documents/publication/wcms_834736.pdf

Tali decisioni devono essere logicamente corrette e tali che, per quanto riguarda la presenza di algoritmi, sfruttati un giusto controllo automatico in merito ai particolari campi di applicazione. L'OIL dà la normale regolamentazione della norma e dell'idea, affermando che gli algoritmi pongano un giusto controllo sui dati anche a fine della ridefinizione del rapporto di lavoro. L'incentivo di miglioramento indotto dal sistema informatico pone l'idea della "performance", intesa in senso lato, non a scapito della "dignità umana". Da questo punto si considera la regolamentazione data dai sindacati, dunque parlando dei "social partners" secondo l'*European social partners framework agreement on digitalisation*.

Le piattaforme digitali non trattano dati che non siano connessi e strettamente necessari, in particolare non dovendo possedere informazioni connesse allo stato emotivo e psicologico del lavoratore. In questo senso, il framework di prima (nel giugno 2020) stabilisce delle misure minime di protezione, focalizzandosi sulla *minimizzazione* e sulla *trasparenza* di quali dati siano raccolti, permettendo ai lavoratori e ai loro rappresentanti di far emergere problematiche legate ai dati, alla loro gestione/sorveglianza/protezione. Importante in conclusione rendere un giusto bilanciamento tra la profilazione/monitoraggio dati, tali da raggiungere il concetto di *potenziamento umano* (uomo tutelato ed aiutato, nei giusti limiti dalla macchina, non disumanizzato).

L'idea è quindi la minimizzazione dei dati raccolti e trattati; infatti, il *management algoritmico* è disciplinato dalla direttiva 2021 (da art. 6 a 10) della proposta di direttiva 2021 del parlamento europeo, al fine del possibile miglioramento delle condizioni di lavoro e di obbligo di informazione. Si ritiene trattamento necessario; se non necessario, naturalmente, si pone il bisogno di consenso. Essendo gli algoritmi, infatti, dei mezzi di valutazione delle prestazioni dei lavoratori, bisogna porre attenzione "a ciò che non viene fatto dagli umani". Essendo ogni persona capitale, ciascuna può essere meramente valutata come oggetto, di produzione ma anche di creazione di risorse economiche, in maniera coordinata ed organizzata dall'alto, perdendo di fatto lo scopo di performance iniziale e di migliore organizzazione con cui la maggior parte di questi è stata creata.

Arriviamo quindi all'introduzione del rapporto di lavoro; anch'esso necessita di una seria regolamentazione, rapportata bilateralmente, in ogni sua forma (più "fumose", come gli stage, attività formative tutelate dalle Regioni, quelle senza scopo di lucro, associazioni e/o volontariati quindi, fino alle "classiche", dove per ognuno si guarda al diritto di lavoro, ferie, consulenza, ecc.).

La macchina quindi pone controllo sull'umano, usando strumenti elettronici per valutarne il lavoro e la performance, ma deve esservi posto un limite (non trattano dati personali se non *connessi e strettamente necessari allo scopo dell'attività*, in particolare, non si trattano dati relativi allo stato *emotivo e psicologico del lavoratore*). Tale principio di dato definito necessario vale, parallelamente, anche per il controllo che viene posto da parte delle piattaforme digitali.

Subordinazione/autonomia

Vediamo quindi come l'ordinamento italiano coordina, assieme all'Unione Europea, l'*autonomia*. Nel corso del tempo si sono aggiunte una serie di modifiche normative in modo scoordinato, rendendo il tutto molto complesso. Ad esempio, la regolamentazione per un libero professionista, la stipulazione dell'accordo tra l'agenzia e il cliente, contratti d'appalto con privato e varie casistiche.

L'UE regola il *distacco intracomunitario*, permettendo la prosecuzione del rapporto di lavoro tra stato membro UE e una specifica impresa facente parte.

Cosa distingue dunque le varie forme di libertà professionale legata alle forme di istituzione e di mercato? Il diritto del lavoro si muove in una direzione opposta rispetto al resto delle forme di diritto, dato che le clausole non sostituiscono le norme inderogabili (quindi il contratto è vincolato alla norme minime orarie e di stipendio, al fine di atto anticoncorrenziale, protettivo della parte debole lavoratore).

Vi deve essere quindi simmetria di relazione, in quanto considerabile potenzialmente ostile e sbilanciabile a favore di una delle due parti, non avendo equa partecipazione. Chi è dunque considerabile destinatario di tali pratiche anticoncorrenziali, tra chi effettivamente lavora e chi norma il lavoro stesso?

Le norme giuridiche descrivono chi è il prestatore di lavoro come persona, in maniera *obbligatoria e vincolata* da un contratto, collaborando nell'attività d'impresa e creando un modello organizzativo quantomeno teoricamente. Viene definito imprenditore "*chi esercita professionalmente un'attività economica organizzata al fine della produzione o dello scambio di beni o di servizi*". Le norme di distinzione tra operaio ed impiegato risalgono al 1924, distinguendo chi esegue lavoro manuale da chi si pone "intellettualmente" ad eseguire la stessa professione.

Il lavoratore deve attenersi ad ordini e direttive, con un principio definito come *eterodirezione* per gli scopi aziendali, a prescindere dal tipo di contratto e possibile rapporto di lavoro.

In effetti le norme come primo scopo si pongono oggettivamente la protezione della sicurezza di chi gestisce il potere direttivo, funzionale agli scopi di impresa e di produzione. Se tali scopi non vi sono, l'ordine è *illegittimo*, in quanto il vincolo di dipendenza va oltre a cosa sia effettivamente necessario (ad esempio assunzione dipendenti in base a vincoli estetici, ad esempio non accettando dipendenti con piercing/tatuaggi).

In generale, un *prestatore di lavoro subordinato* è definito secondo l'art. 2094 c.c come "*chi si obbliga mediante retribuzione a collaborare nell'impresa, prestando il proprio lavoro intellettuale o manuale alle dipendenze e sotto la direzione dell'imprenditore*".

Tutto ciò si pone di fronte ad un vincolo di accettazione del contratto, rispettando gli ordini direttivi del datore di lavoro. Il datore di lavoro viene quindi condannato al risarcimento del danno nel caso di vincoli non richiesti e il lavoratore ha diritto di chiedere al giudice l'annullamento di vincoli non legittimi. Il rapporto di lavoro non è sottoponibile a discussione (ad esempio discriminazione nei confronti di una donna, con diritto di reintegra a seguito di esclusione per futili motivi, classico esempio donna incinta).

Il lavoratore può far valere i propri diritti (*esecuzione coattiva*), per cui a livello legale esistono sentenze ed atti in grado di avvalorare le tesi di diritto, non potendo imporre obblighi precisi anche allo stesso datore di lavoro; tuttavia, i rapporti di lavoro subordinato, devono rispondere alle disposizioni presenti dalle sezioni II, III, IV del capo I del titolo II, in quanto compatibili con la specialità del rapporto (*articolo 2239, norme applicabili*).

Senza vincolo di subordinazione, può essere regolato il fornimento di opera/servizio, senza obbligo di collaborazione ma di esecuzione di un'opera/servizio prevalentemente proprio (distaccandolo considerevolmente dal lavoro autonomo, *articolo 2222 c.c/contratto d'opera*), non avendo obbligo di comando/orario/indicazione perché *non vi è un vincolo di subordinazione*. Il legislatore specifica diverse

terminologie (persona, esecutore, ecc.) per descrivere il lavoratore, mettendo in evidenza che non si specifica il rapporto tra persone ma tra imprese, assumendo in maniera onerosa una corresponsività di esecuzione e di gestione del rapporto, *articolo 1655 c.c./contratto d'appalto-nozione*, (contratto in cui una parte assume, con organizzazione dei mezzi necessari e con gestione a proprio rischio, il compimento di un'opera o di un servizio verso un corrispettivo in denaro, pena pagamento di penali se si violassero accordi/vincoli particolari presenti alla base).

Con degli specifici vincoli (es. orario, garanzia di fatto di vincolo di subordinazione) si distingue il contratto d'opera da quello d'appalto. L'organizzazione dei rapporti interni all'azienda e approccio esterno all'usufruttore di servizio è in mano alla stessa azienda e di fatto, tale che sussistono regole interne e gestiscono il rapporto pubblico con il cliente. Ad esempio, anche la fornitura di un servizio di sicurezza, fornito ad un ente esterno, un amministratore gestisce all'interno dell'azienda la regolamentazione ed effettiva applicazione che può essere considerato illegale nel caso in cui non vengano adempiuti gli scopi contrattuali/legali (l'amministratore che si sostituisce al regolatore esecutivo del rapporto di lavoro, quindi l'appaltatore, è vincolato).

L'ordinamento ammette che possano essere impartiti ordini definibili "giusti", evitando casi di caporalato. L'appalto è una forma particolare per la sua duplice natura a doppio taglio; quindi, per quanto descritto si potrebbero avere problematiche di applicazione e rispetto delle stesse norme.

Si osserva poi il caso particolare delle, citando *l'art. 409 del Codice di procedura civile* (c.p.c, qui scritta perché dispongono di un sistema processuale autonomo a sé stante, con processi agevolati e poco durevoli), quindi le *controversie individuali di lavoro*, applicabili ai lavoratori subordinati (art. 2099 c.c.) anche se non inerenti all'esercizio di un'impresa (art. 2239 c.c) e, similmente, ai rapporti d'agenzia (art. 1742 c.c.), di rappresentanza commerciale ed altri che si "*concretino in prestazione di opera continuativa e coordinata prevalentemente personale anche se non a carattere subordinato*", come le Co.co.co (Collaborazioni coordinate e continuative).

Nel caso di queste ultime, si ha un accordo basato sull'autonomia (il lavoratore decide tempi e modalità di esecuzione), continuo (per i termini temporali stabiliti dal vincolo contrattuale), secondo un principio di collaborazione occasionale. Il pagamento è un compenso mensile senza vincoli di orario. La tutela è incisiva, e stabilita ai rapporti di lavoro subordinati e ai rapporti di agenzia, concretizzati in prestazioni continuative, coordinate e personali. Si intende coordinata "*una collaborazione rispetto a modalità di collegamento e accordo comune tra le parti ed il collaboratore organizza autonomamente l'attività lavorativa.*" Grazie al Jobs Act, la disciplina del lavoro subordinato di applica anche alle Co.co.co, estendendo le norme presenti in questo senso.

Controversie individuali e potere direttivo (lavoro subordinato)

La collaborazione continuativa coordinata equipara il lavoratore subordinato al lavoratore con poteri direttivi, prendendo l'esempio della norma che cita il punto *dell'organizzata autonomamente*, non essendoci un potere unilaterale e *di comune accordo*.

La base è *l'etero organizzazione*, in quanto organizzata dal committente ma il rapporto resta quantomeno doppio. La piattaforma digitale si occupa di gestione di programmi e procedure anche informatiche, con una propria regolamentazione di discipline/servizi. In tutti gli altri casi (assenza di potere direttivo, coordinamento continuativo), vi sono ben poche tutele, nel caso di potere direttivo ci sono tutte le tutele, mentre per beni di ambito urbano, rider, ecc. si applicano tutele ad hoc. Ovviamente essendo lavoro subordinato, le piattaforme fanno il bello e cattivo tempo, specialmente in un'epoca dove si parla di management algoritmico, automatizzando il più possibile la pratica.

Precedentemente si rientrava nell'art. 2222 (quindi lavoratore subordinato autonomo) o nell'articolo 2 d. lgs 81/2015 se vi erano pratiche di organizzazione aziendale, oggi invece esistono norme ad hoc per un certo lavoratore.

Citiamo l'art 47-bis d.lgs. 81/2015, che stabilisce dei livelli minimi di tutela per i prestatori occupati con rapporti di lavoro non subordinato ma che, per esempio, esercitano professione atte alla consegna di beni per conto altrui, in ambito urbano o con l'ausilio di velocipedi o veicoli a motore e anche dei rider, promuovendo un'occupazione sicura e dignitosa ulteriormente, perché sottoposti a controllo diretto di piattaforme digitali (decreto dignità 2019).

Lo stesso articolo dice che "Ai fini del presente decreto si considerano piattaforme digitali i programmi e le procedure informatiche delle imprese che, indipendentemente dal luogo di stabilimento, organizzano le attività di consegna di beni, fissandone il prezzo e determinando le modalità di esecuzione della prestazione". Il modello italiano segue questa direzione (presente anche nella foto)

<ul style="list-style-type: none"> - 2094, prestatore di lavoro subordinato, Tutte le tutele e Presenza del potere direttivo - 2222, Norme applicabili nel lavoro subordinato, Poche tutele e Assenza del potere direttivo - 409, Co.co.co, Poche tutele - Art. 2. D. lgs. 81/2015, Etero-organizzazione, Tutte le tutele - Art. 47-bis D. lgs. 81/2015, Rider e consegne, autonomia, Tutele ad hoc 	<p>Art. 2094 c.c.</p> <p>- Quali sono gli elementi essenziali?</p> <p>Potere direttivo</p> <p>- Quali tutele?</p> <p>Tutte</p> 	<p>Art. 2222 c.c.</p> <p>- Quali sono gli elementi essenziali?</p> <p>Assenza del potere direttivo</p> <p>- Quali tutele?</p> <p>Molto poche (vedi legge 81/2017)</p>	<p>Art. 409 c.p.c.</p> <p>- Quali sono gli elementi essenziali?</p> <p>Continuità coordinamento</p> <p>- Quali tutele?</p> <p>Molto poche (vedi legge 81/2017)</p>	<p>Art. 2 d.lgs. 81/2015</p> <p>- Quali sono gli elementi essenziali?</p> <p>Etero organizzazione</p> <p>- Quali tutele?</p> <p>Tutte</p> 	<p>Art. 47-bis d.lgs. 81/2015</p> <p>- Quali sono gli elementi essenziali?</p> <p>Rider, velocipede, consegna beni in ambito urbano, autonomia</p> <p>- Quali tutele?</p> <p>Pacchetto ad hoc</p>
--	--	--	---	---	--

Approfondiamo il potere direttivo, impartendo regole secondo un vincolo di *assoggettamento continuativo e sistematico* dando ordini precisi e tassativi sull'organizzazione della prestazione professionale, capendo quali siano giustificati dall'ordine aziendale, conformando le modalità di svolgimento della prestazione. Il potere è unilaterale e stabilisce *ordini precisi e tassativi*, in merito all'organizzazione aziendale preesistente.

A questo scopo si analizzano possibili figure controverse, partendo dai dirigenti, giornalisti, insegnanti, medici, telelavoro, pony express/posta prioritaria, propagandisti/rappresentanti, pulizia di locali, ecc.). In questo senso, chiaramente, entrano in vigore direttive specifiche/regolamenti ad hoc, ma sono tutte figure che non dispongono di un controllo inteso in senso tradizionale oppure di un senso di autonomia dato dalla stessa natura della professione.

Di fatto si segue l'articolo 2104 (*diligenza del prestatore di lavoro*), per cui il lavoratore deve usare la propria diligenza per applicare le giuste direttive in base anche alla sua posizione gerarchica, nonché la competenza di affari, per conto proprio/terzi, non entrando in concorrenza con il proprio imprenditore (art. 2105, *obbligo di fedeltà*), anche per motivi di privacy (possiede infatti informazioni sensibili). Vengono quindi applicate sanzioni disciplinari a seconda del tipo di violazione/infrazione nel contesto specifico e in base alla gravità dell'atto (secondo l'art. 2106, *sanzioni disciplinari*). Esse vanno applicate secondo un principio di proporzionalità tra infrazione e sanzione.

Vediamo il caso di un mulettista (video) che distrugge tutto lo stabilimento per manovra sbagliata: il lavoratore può porre un provvedimento disciplinare, per mancanza di corretta formazione per l'esecuzione del proprio lavoro. Si apre una possibile fase di contestazione e si cerca di capire l'imputabilità della responsabilità di azione. In questo caso, di per sé, il datore di lavoro può esercitare il proprio potere disciplinare in varie modalità, in particolare, citando l'art. 2087 c.c., "l'imprenditore è tenuto ad adottare

nell'esercizio dell'impresa le misure che, secondo la particolarità del lavoro, l'esperienza e la tecnica, sono necessarie a tutelare l'integrità fisica e la personalità morale dei prestatori di lavoro".

L'articolo 7 dello Statuto dei Lavoratori dice che deve essere elaborato un codice disciplinare, riguardando nel nostro caso la violazione di procedure informatiche, ma anche l'entità delle sanzioni disciplinari, da un punto di vista di procedure, multe, sospensioni e possibili *impugnazioni* (approfondite sotto). Naturalmente le procedure organizzative rientrano in parte nel buon senso (possibilmente comunque disciplinato da un regolamento aziendale) per cui non può essere contestato inadempimento, evidenziando le regole/sanzioni assunte in caso di violazione.

Potere disciplinare e diritti sindacali

Partendo proprio dalla definizione, il potere disciplinare pone i giusti limiti procedurali e l'entità delle sanzioni disciplinari al lavoratore in merito a comportamenti inadempienti (nel caso di contratti si provvede alla risoluzione). Si può discutere di una multa (trattenuta di 4 ore massime di stipendio) oppure la sospensione, quindi il datore di lavoro rifiuta la prestazione del lavoratore e non pagandola, per un massimo di 10 giorni (*regime delle impugnazioni*, quindi discutere se una ordinanza sia illegittima o meno, dipendentemente dal contesto applicativo).

Il lavoratore in questo caso ha diritto a costituire un collegio di scelta o un arbitrato, anche in senso all'azienda, vincolando alla nomina il datore di lavoro e la multa non può essere disposta per un importo superiore a quattro ore della retribuzione base e la sospensione dal servizio e dalla retribuzione per più di dieci giorni.

Il datore deve elaborare un codice disciplinare, il quale deve essere affisso in luogo visibile, individuando quali sono i limiti posti e le regole fondamentali da seguire ed osservare, nonché le sanzioni ponibili in caso di violazione. Il datore di lavoro quindi deve essere posto a regolamentazione. Tutto ciò che appartiene all'organizzazione dell'impresa, compresa la regolamentazione informatica.

La lingua in cui questo è scritto, per il regolamento della privacy, si concentra sul principio di trasparenza, veicolando quantomeno il regolamento in inglese e ponendo attenzione all'obiettivo.

Ai contratti collettivi si pongono attenzioni particolari, ove applicabili, per esempio nei casi dei contratti sindacali (posti a tutela di una certa categoria), applicabile ai lavoratori subordinati. Secondo l'*articolo 2103* comma 1, si parla di mansione, quindi l'oggetto del contratto di lavoro *subordinato* (negli altri contratti l'oggetto è l'opera o il servizio), corrispondenti al suo inquadramento o commisurato alle sue competenze, rispettando la professionalità specifica del lavoratore, legalmente inquadrando le ultime attività effettivamente svolte. Le mansioni fanno parte a livelli delle declaratorie contrattuali, rinviando la contrattazione collettiva e raggruppando i singoli impieghi in generiche macrocategorie.

La *categoria* ingloba il *livello*, cioè:

- operai
- impiegati
- quadri intermedi (categoria intermedia tra impiegati di alto livello e i dirigenti)
- dirigenti

Il datore di lavoro può adibire il lavoratore ad una funzione più alta (che può non accettare per stress/responsabilità, ecc.), dando diritto alla promozione (ma anche l'adibizione a mansioni inferiori, con limitazioni; si può scendere solo di un livello quando ragioni oggettive dell'azienda lo giustificano, non ragioni soggettive del datore di lavoro). Previo consenso, il lavoratore accetta non solo le promozioni ma anche modifiche peggiorative, se risponde a motivi personali/ragioni soggettive del lavoratore, purché la

modifica sia avallata da una commissione pubblica, attestante che il lavoratore sia effettivamente libero nella scelta.

Nell'ambito professionale, non si vede la mansione ad uno scopo di formazione, quanto piuttosto di sola produttività (vincolante l'autonomia imprenditoriale, quindi anche giuridicamente l'azienda è mezzo economico e non di apprendimento diretto).

Comunque, il comma 1 dell'articolo 2103 c.c. cita che il lavoratore venga "assunto per mansioni corrispondenti a quelle per cui è stato assunto oppure all'inquadramento superiore che ha successivamente acquisito rispetto a mansioni riconducibili allo stesso livello/categoria legale di inquadramento delle ultime svolte".

Si cita il comma 7 dell'articolo 2103 c.c.:

"Nel caso di assegnazione a mansioni superiori il lavoratore ha diritto al trattamento corrispondente all'attività svolta e l'assegnazione diviene definitiva, salvo diversa volontà del lavoratore, ove la medesima non abbia avuto luogo per ragioni sostitutive di altro lavoratore in servizio, dopo il periodo fissato dai contratti collettivi o, in mancanza, dopo sei mesi continuativi". Similmente, il lavoratore non può essere trasferito da un'unità produttiva ad un'altra se non per comprovate ragioni tecniche, organizzative e produttive.

L'accordo deve essere stipulato di fronte ad organismi che il lavoratore intende accettare limiti di mansionamento e tutela dell'occupazione sulla base della professionalità. Anche nel caso di inabilità/disabilità si discute la mancanza di capacità possibile per il lavoratore nell'accordo di contratto, con regolamento transitorio tra fase pre e post contratto.

Nel caso di trasferimento, similmente, non è possibile adibirlo se non per ragioni oggettive (*giusta causa* nel caso di trasferimento oltre i 50 Km, riconoscendo solo in questo caso la tutela di disoccupazione involontaria, la NASpl, prevista inoltre solo nel caso di licenziamento).

Giustamente il contratto vincola il lavoratore fino alla scadenza relativa, per cessazione naturale del contratto e né il datore né il dipendente possono abusarne, il primo lasciando a casa il dipendente a propria volontà, il secondo rimanendo a casa volontariamente per molto tempo senza cause motivabili. Nel caso dei *contratti atipici* (voucher, stage, lavori intermittenti, orari ridotti/flessibili, somministrazione di lavoro), si ha una regolamentazione non espressamente disciplinata dal diritto civile, ma viene creata ad hoc dalle parti (volontà inter-partes).

Ci deve essere quindi un giustificato mancamento soggettivo nel caso di licenziamento, che non sono inadempimenti ma incidono sul vincolo giudiziario. È quindi delicato cercare di capire tutta la situazione. La giusta causa si riferisce all'articolo 2119 del Codice civile, quindi:

"Ciascuno dei contraenti può recedere dal contratto prima della scadenza del termine, se il contratto è a tempo determinato, o senza preavviso, se il contratto è a tempo indeterminato, qualora si verifichi una causa che non consenta la prosecuzione, anche provvisoria, del rapporto. Se il contratto è a tempo indeterminato, al prestatore di lavoro che recede per giusta causa compete l'indennità indicata nel secondo comma dell'articolo precedente. Non costituisce giusta causa di risoluzione del contratto il fallimento dell'imprenditore o la liquidazione coatta amministrativa dell'azienda.". Nota di contorno, in questo rientra anche il possibile blocco per Covid (altre leggi di riferimento sono la legge 604/1966 (licenziamento civile per giusta causa), l'Art. 18 St. lav. (risarcimento del danno subito a causa del licenziamento), la legge 223/1991 (cassa integrazione, mobilità), D.lgs. 23/2015).

La fiducia va posta in primis nella regolamentazione del rapporto di lavoro e quindi della sua capacità ad eseguire correttamente quella specifica prestazione con caratteristiche stabilite e concrete in un certo campo applicativo. Anche nel caso di pregiudizio viene richiesto in maniera specifica il certificato dei carichi pendenti (ovviamente utile nel caso di mansione di ordine e/o sicurezza). L'attività lavorativa non viene preclusa a chi si macchia di reati, normalmente.

Scritto da Gabriel

Quali sono le informazioni utilizzabili dal datore di lavoro per lo svolgimento della professione? Vengono posti esempi di costruzione di un profilo psicologico/sanitario, facendo possibilmente delle verifiche medico-sanitarie sulla base della specifica mansione, avendo delle prescrizioni oggettive ma non chiarendo la loro logica di applicazione.

In ultimo ai lavoratori viene principalmente data tutela tramite l'art.39 (tutela giuridica da parte di associazioni sindacali), art.40 (diritto di sciopero), art. 41 (iniziativa economica privata è libera, non recando danno sociale) e lo Statuto dei Lavoratori (per approfondire metto: https://www.cgil.unimi.it/wp-content/uploads/2014/01/I_300_70.pdf)

Oltre a questi si citano anche i titoli 1/2 (i titoli contengono gli articoli) con applicazione generalizzata e in particolare attenzione agli articoli 1-6, 8, 14, 15-17 dello stesso statuto. (Link apposito di consultazione: <https://www.altalex.com/documents/codici-altalex/2014/10/30/statuto-dei-lavoratori>)

Per le aziende più grandi si prevede la regolamentazione dell'articolo 35 dello stesso, quindi rappresentanze sindacali, assemblee, trasferimento dirigenziale di RSA, permessi retribuiti e no, diritto di affissione, contributi sindacali e locali delle RSA.

Diritto del lavoro: lavoro e persona

Si pone il dubbio di come il lavoratore sia controllato rispetto al proprio datore di lavoro, in merito soprattutto a come vengono trattate le sue informazioni personali. Si valutano quindi le attitudini e gli atteggiamenti di un certo candidato/lavoratore, al controllo della sicurezza oppure di sanità mentale dello stesso. In generale si parla di qualsiasi fatto/aspetto non direttamente collegato all'attitudine professionale, tutelando la riservatezza del lavoratore in maniera oggettiva, secondo l'articolo 8 dello statuto dei lavoratori (valente sia prima della stipulazione del rapporto di lavoro sia durante l'esecuzione dello stesso). Si ha anche il diritto di obiezione, dove il lavoratore può in maniera legittima, tutelare i propri interessi (idee politiche, idee religiose, orientamento sessuale, ecc.) o anche, nel caso di una donna, il fatto di avere figli/famiglia, ecc.

Un'obiezione valida si pone solo nel caso di tutela; ad esempio, nel caso di domande in merito all'organizzazione dei posti di lavoro e relativa sostituzione di un certo lavoratore, non astenendosi per il futuro dal rapporto lavorativo. Chi non venisse assunto potrebbe fare riferimento ai decreti delle pari opportunità, aspirando solo ad un possibile risarcimento, non ad una riassunzione forzata.

È possibile registrare anche un datore di lavoro, a tutela dei propri interessi, come possibile riprova della propria testimonianza di "giusta causa". Solo nel caso ad esempio di licenziamento con comportamento lesivo, il datore di lavoro è obbligato alla reintroduzione del lavoratore e anche al pagamento delle mensilità.

Si deve quindi capire il senso della limitazione, nel contesto dell'attività produttiva: al datore di lavoro potrebbe non interessare il fatto di avere piercing, trucco oppure una particolare capigliatura. Ci sono particolari esigenze di igiene/sterilizzazione, esempio ristorazione, criteri oggettivi di comportamento consentito di tutela dell'interesse professionale da parte del datore di lavoro. Non tutti i regolamenti aziendali risultano legittimi, chiaramente.

Anche l'uso di Internet è un discorso complesso; citiamo l'esempio di una particolare sentenza, sentenza Barbulescu. Un ingegnere rumeno dipendente di una Società privata veniva licenziato per ragioni disciplinari poiché sorpreso ad utilizzare per scopi personali l'account messenger aziendale, pur sapendo che il regolamento interno vietava ogni uso privato degli strumenti aziendali.

L'ex dipendente conveniva in giudizio la società datrice di lavoro per chiedere l'accertamento della illegittimità del licenziamento, eccependo una ingiustificata ingerenza nella propria vita privata e, quindi, una violazione della normativa sulla privacy.

Secondo i Giudici di primo grado, il licenziamento era legittimo non sussistendo alcuna violazione della privacy. Avverso la sentenza di primo grado, il lavoratore proponeva appello che veniva respinto (perché la Romania, paese di giudizio, non prevedeva regolamentazioni in merito alla privacy). Il lavoratore decideva, allora, di rivolgersi alla Corte Europea dei Diritti dell'Uomo.

Il caso veniva assegnato alla IV sezione della Corte che, con sentenza 12 gennaio 2016, si pronunciava in favore dell'azienda, non ritenendo il controllo sulla posta elettronica del dipendente in contrasto con l'art. 8 della Cedu.

Il lavoratore propone appello dinanzi alla Grande Chambre e la sentenza di primo grado viene riformata. Secondo la Grande Chambre, i giudici nazionali non avevano operato un corretto bilanciamento tra gli interessi in gioco, vale a dire, da un lato, l'interesse del datore di lavoro al corretto funzionamento dell'azienda e, dall'altro, quello del lavoratore alla salvaguardia della propria vita privata. Ampliando il concetto di "privacy" del lavoratore, la sentenza ha stabilito che la vita privata del lavoratore sul luogo di lavoro non può essere ridotta a "zero", per cui le comunicazioni trasmesse sul posto di lavoro rientrano nel concetto di "vita privata" e di "corrispondenza" tutelati dall'art. 8 della Cedu.

A questo si collega anche il regolamento europeo in materia di privacy, ponendo divieto anche in merito all'articolo 8, che vieta *"al datore di lavoro di effettuare indagini, anche a mezzo di terzi, sulle opinioni politiche, religiose o sindacali del lavoratore, nonché su fatti non rilevanti ai fini della valutazione dell'attitudine professionale del lavoratore"*.

Tutto dipende dall'oggetto, dal contesto e dai fini dello stesso contratto di lavoro. Chiaro quindi come la tecnologia si intenda sia come i dispositivi/applicazione che li fanno funzionare, sia le caratteristiche incorporate nell'architettura tecnologica, divergendo per caratteristiche tecniche, funzionali e di immagazzinamento dei dati. Non è possibile contestualizzare un certo comportamento facente parte della vita privata del lavoratore e sfruttarlo come pretesto per poter effettuare pressioni su di lui.

La tecnologia incorpora, per sua definizione, funzionalità di controllo e sorveglianza e le tipologie di controllo esercitato divergono in relazione a caratteristiche tecniche, modalità ed ambiti di potenziale esplicazione, oltre che in relazione alla possibilità riconosciuta dell'utente di attivarne/disattivarne le funzioni (nonché consapevolezza delle modalità di immagazzinamento dei dati).

L'installazione ad esempio di videocamere si pone nel caso di videosorveglianza, furti, sicurezza; tuttavia, dato che si possono usare tali strumenti per verificare l'operosità dei propri impiegati, alcuni limiti sono posti dall'articolo 4 dello Statuto dei Lavoratori.

Da questo si discute l'utilità di idee come *BYOD/T/P/PC (Bring Your Own Device/Technology/Phone/PC)*, *WYOD (Wear Your Own Device)*, permesso dal comma 4 dell'articolo 4 dello Statuto dei Lavoratori, non chiedendo accordi ai sindacati o al legislatore sulla validità di strumenti non necessariamente per scopi lavorativi.

Parliamo di una modalità di svolgimento della prestazione lavorativa concordata, cioè lo *smart working*, dove il lavoro viene svolto fuori dall'azienda e definito gergalmente come "lavoro da casa" (tutelata dalla legge 81 del 2017, comunque già preesistente).

Viene stabilito infatti che il lavoro possa essere svolto *anche* fuori dall'azienda; si possono stabilire le stesse modalità di svolgimento telematiche, ai fini di non violazione della libertà personale.

Gli strumenti tecnologici raccolgono dati di continuo, intercettando ogni nostra azione. *Le possibili tipologie di controllo divergono in relazione a caratteristiche tecniche, modalità ed ambiti di potenziale esplicazione,*

oltre che in relazione alla possibilità riconosciuta all'utente di attivarne/disattivarne le funzioni (consapevolezza circa le modalità di immagazzinamento dei dati sull'attività lavorativa: nuovo art. 4 St. lav.)

Limitando nell'accordo di lavoro l'utilizzo di strumenti, limito il controllo da parte dei datori di lavoro. Dunque, è delicato, soprattutto ai fini della sicurezza, in merito agli strumenti forniti dallo stesso. In casi particolari come quelli della pandemia, l'accordo unilaterale di smart working veniva imposto, ma normalmente è in vigore la normativa ordinaria che richiede regolare accordo.

È insito nell'ambito dell'accordo di lavoro, soprattutto in ambito autonomo o di libera dipendenza (freelance, partita IVA, ecc.) come sia indipendente dal luogo e dalla regolamentazione di smart working del lavoro e della professione. Chiaramente il lavoratore è la parte debole, dato che non ha molto margine di intervento; infatti, in merito allo *smart working*, il poter lavorare da casa è una semplice possibilità, alternativa, alla normale regolamentazione della pratica.

Nell'accordo individuale che stabilisce quali siano i dispositivi utilizzati, vengono anche regolamentati i tempi di riposo del lavoratore, nonché le forme di controllo e di potere direttivo posto dalla figura del datore di lavoro, anche in merito a provvedimenti disciplinari (chiamando anche in causa la contrattazione collettiva). In questo caso specifico, la regolamentazione viene offerta dall'articolo 4 dello Statuto dei Lavoratori, non ponendo un deciso controllo su strumenti come caselle aziendali/e-mail. Si pronuncia, oltre al principio di raccolta di soli dati considerati utili allo svolgimento dell'attività di lavoro, anche il diritto alla disconnessione, stabilendo delle giuste pause in maniera corretta ed esplicita.

Lavoro, persone e tecnologie

L'idea della sentenza Barbulescu è di confrontare l'idea di un dipendente che usava gli strumenti tecnologici a scopo proprio. Si pone il dubbio di quanto i contatti elettronici siano spiabili, come è stato nel caso del Barbulescu e di quanto la "corrispondenza chiusa" sia fonte di informazioni private del lavoratore, dimostrando che i mezzi di produzione siano stati installati nel rispetto delle condizioni professionali.

Il regolamento aziendale pone consapevolezza al lavoratore di quanto egli debba essere consapevole di quali ritorsioni e diritti possa avere. Citiamo l'articolo 8 della Carta dei Diritti dell'Uomo:

1) "Ogni individuo ha diritto al rispetto della propria vita privata e familiare, della propria casa e della propria corrispondenza."

2) "L'ingerenza di un'autorità pubblica nell'esercizio di tale diritto può essere ingerenza solo nella misura in cui tale ingerenza sia prevista dalla legge e costituisca una misura necessaria, in una società democratica, per la sicurezza nazionale, la sicurezza pubblica, il benessere economico del Paese, la difesa dell'ordine e la prevenzione di reati, la protezione della salute o della morale, o la protezione dei diritti e delle libertà altrui."

Di fatto la libertà di impresa è condizionata anch'essa in maniera libera, autodisciplinandosi, dall'articolo 41 della costituzione, in base al comma "L'iniziativa economica privata è libera".

È libera, ma "non può svolgersi in contrasto con l'utilità sociale o in modo da recare danno alla salute, all'ambiente, alla sicurezza, alla libertà, alla dignità umana". La nostra costituzione, all'articolo 41, stabilisce che ci debba essere un giusto bilanciamento tra l'interesse produttivo/organizzativo dell'impresa e la dignità del lavoratore e/o dei soggetti coinvolti.

Da questo punto di vista si discutono le finalità di utilizzo e modalità d'uso dei dati trattati, capendo quali siano i soggetti preposti alla tutela. Ad esempio, l'installazione di videocamere, giustificata come tutela da atti criminosi dei dipendenti. È veramente giusto o è violazione della privacy? Come discusso dallo stesso articolo, le nuove tecnologie, poste a scopo di strumentizzazione/organizzazione produttiva devono essere sempre poste al rispetto della dignità dei singoli e delle parti presenti.

Citiamo l'articolo 29 del regolamento UE: *“Il responsabile del trattamento, o chiunque agisca sotto la sua autorità o sotto quella del titolare del trattamento, che abbia accesso a dati personali non può trattare tali dati se non è istruito in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri.”*

La problematica si ha nella corretta definizione di tre aspetti tra loro correlati:

- le finalità di utilizzo dei dati raccolti
- le modalità d'uso dei dati trattati
- la definizione dei soggetti preposti all'utilizzo dei dati

Devono quindi essere creati dei regolamenti chiari, comprensibili, dando le giuste informazioni. In particolare, nell'informatica, il ruolo degli amministratori di sistema è fondamentale e richiede formazione specifica, visto a seconda dell'impresa, il valore dei dati trattati. Da un lato quindi si cerca di capire se l'ordinamento pone limiti ai poteri imprenditoriali, dall'altra però possono emergere dei ruoli che hanno un potere con margini ampi e non ben definiti.

L'articolo 6 del GDPR (<https://www.altalex.com/documents/news/2018/04/12/articolo-6-gdpr-liceita-del-trattamento>) pone i giusti limiti/tutele del controllore di questi dati, affinché si abbia *bilanciamento per l'interesse dei diritti/libertà fondamentali sui dati*. Fondamentalmente l'articolo racchiude tutto quanto sia stato finora discusso. È chiaro quindi come gli interessi debbano essere bilanciati tra le parti, in nome del rispetto dei diritti fondamentali e delle libertà dei dati.

Le informazioni sensibili vanno quindi tutelate; citiamo il caso Copland vs. The United Kingdom, contenzioso tra impiegata amministrativa e università, con intercettazione dei messaggi privati, ammettendo che *“il monitoraggio dell'uso del telefono/e-mail/Internet da parte di un impiegato nel posto di lavoro sia considerato necessario in certe situazioni per uno scopo legittimo”*, quindi di controllo della propria lavoratrice. Similmente, si riporta il caso di una segretaria amministrativa di uno Studio professionale, licenziata per utilizzo del computer aziendale a fini privati, contestando un totale di 6000 accessi negli ultimi 18 mesi a social network/giochi/musica ed app non connesse all'attività lavorativa.

Strumenti di lavoro e accordi/vincoli nel loro utilizzo

Citiamo altri due casi:

- tribunale di Brescia, sentenza del 2016. Il datore di lavoro si è limitato a stampare la *cronologia* ed il tipo di accesso ad internet dal computer della dipendente: questo non richiede l'installazione di alcun dispositivo di controllo né implica la violazione della privacy, trattandosi di dati che vengono registrati da qualsiasi computer e che sono stati stampati al solo fine di verificare l'utilizzo di uno strumento messo a disposizione dal datore di lavoro per l'esecuzione della prestazione. Né può ipotizzarsi una violazione dell'art. 4 St. lav., trattandosi di attività di controllo non della produttività ed efficienza nello svolgimento dell'attività lavorativa, ma attinenti a condotte estranee alla prestazione
- tribunale di Napoli, ordinanza del 2014. Il datore di lavoro non ha provveduto a fornire dati attendibili e quindi non ha adempiuto al proprio preciso onere che certo non muta nella sua essenza in ragione del tipo di documenti o dati da esaminare ... ed infatti tutti e due i tipi di *file di log* sono andati distrutti nei loro originali in quanto pacificamente sovrascritti, non conservati nel sistema di archiviazione. Le copie degli stessi non sono state estratte con modalità tali da garantirne, in caso di contestazione, la attendibilità e provenienza e la immodificabilità, né cristallizzati giuridicamente e processualmente in altro modo (consulenza tecnica preventiva/ctp, accertamento tecnico preventivo/atp, cioè un procedimento cautelare che serve a determinare le cause tecniche oggettive che hanno determinato un vizio. ecc.)

Oltre ai testi/articoli citati sopra, si può fare riferimento al *Codice privacy (d. lgs. 196/2003)*, *articoli 2/15/32/41 comma 2 della Costituzione*, *convenzione 108 del 1981* (tutela dei dati automatizzati e corrispondenti al cittadino), *Direttiva 95/46/CE* (garanzie generali superanti le limitazioni interne all'UE, anche in materia libertà personale), lo stesso GDPR oppure anche la *direttiva 2002/58/CE* (stabilendo completamente i dispositivi, la riservatezza delle comunicazioni e le varie norme tra le aziende), *articolo 8 Cedu (Convenzione Europea per la salvaguardia dei Diritti dell'Uomo)* (ogni persona ha diritto al rispetto della propria vita privata e familiare, del proprio domicilio e della propria corrispondenza). Potenzialmente la libertà personale viene violata, dato che l'esito del controllo è significativo in merito alla gravità del comportamento del dipendente.

Il prof evidenzia queste linee in merito alla sentenza in oggetto, con questo riferimento da parte del datore di lavoro (tradotto e riscritto):

"Siamo rimasti sbalorditi nello scoprire che l'11 settembre 2013 hai deliberatamente lacerato l'avambraccio sinistro, usando pezzi di vetro. Questi fatti - all'origine della tua interruzione del lavoro a causa di un incidente sul lavoro - sono stati ripresi dalla telecamera installata nelle cucine del nostro ristorante e la cui visione è stata effettuata, in tua presenza e in quella di un ufficiale giudiziario, da noi incaricato.

Quest'ultimo ha redatto una relazione, di cui alleghiamo una copia. In altre parole, le lesioni che hai subito l'11 settembre 2013 non sono casuali ma sono il risultato di una lacerazione volontaria da parte tua."

Quindi: lavoratrice che si ferisce volutamente con un pezzo di vetro, pur sapendo ci fossero le telecamere. Ciononostante, vista la violazione alla privacy, viene legalmente riammessa a lavoro visto l'eccessivo controllo posto da parte del datore di lavoro e riconosciuto come lesivo nei confronti della dipendente.

Ci si chiede se è stato correttamente bilanciato l'interesse aziendale, in merito soprattutto alle ragioni dell'impresa ma anche di protezione della riservatezza e della dignità dell'individuo. Il licenziamento risulta illegittimo (non certo a causa del danno auto provocato) ma appunto all'interno si ha la violazione della privacy precedentemente citata che prevale legalmente in merito a questo discorso.

In questo caso ci deve essere un bilanciamento preventivo tra le parti, cita il professore, cioè vengano elaborati i dati raccolti, tenendo ragionevolmente conto in modo equo degli interessi di entrambe le parti interessate, rispettando i principi di protezione di entrambe le parti.

A seguito di una modifica del Jobs Act sull'articolo 4 dello Statuto dei Lavoratori si pone:

- divieto *assoluto* di installazione di strumenti per finalità di controllo a distanza dell'attività del lavoratore
- divieto *relativo* di installazione di apparecchiature richieste da esigenze organizzative, produttive, di sicurezza del lavoro o la possibilità di controllo a distanza dell'attività dei lavoratori (forma di controllo preterintenzionale)

Il divieto non opera in caso di caso di installazione previo accordo di strutture sanitarie (RSA) oppure in accordo con le direzioni territoriali del lavoro (DTL). Comunque, l'ambito di controllo giuridico è posto alla liceità del controllo, interpretando in modo estensivo tutte le norme citate/viste/vigenti.

Piccola parentesi sul *Jobs Act*. I contenuti principali sono:

- l'introduzione del contratto a tempo indeterminato a tutele crescenti e la possibilità da parte del datore di lavoro di licenziare un lavoratore dipendente senza giusta causa, prevedendo l'applicazione dell'articolo 18 dello statuto dei lavoratori dopo i primi tre anni di rapporto, ma la reintegrazione nel posto di lavoro viene limitata ad alcuni casi particolari, venendo sostituita in generale dal diritto ad ottenere una indennità a titolo di risarcimento.
- la rimodulazione dei contratti di lavoro dipendente esistenti in Italia;
- la creazione della NASpI (Nuova Assicurazione Sociale per l'Impiego);
- piano di incentivi e decontribuzione per le imprese per favorire le assunzioni a tempo indeterminato, con ammortizzatori sociali utili
- semplificazione dei criteri utili per l'alternanza scuola-lavoro
- creazione dell'Agenzia Nazionale Politiche Attive del Lavoro (Anpal)

Il comma 1 art. 23 del d.lgs. 151/2015 cita come gli strumenti da cui derivino possibilità di controllo a distanza possono essere impiegati *esclusivamente per esigenze organizzative/produktive per sicurezza/tutela del patrimonio aziendale*, previo accordo di RSU/RSA. Il Nuovo articolo 4, comma 1 cita che si deve avere previa autorizzazione rispetto alle singole entità produttive, in mancanza di accordo da parte della sede territoriale dell'INL (Ispettorato Nazionale Lavoro) o per imprese dislocate in varie sedi, di fare riferimento alla sede centrale dell'INL per ogni casistica così descritta.

A questo livello, occorre un accordo sindacale per ogni computer/programma utilizzato nel nostro ambito. Tuttavia, il comma 2 fornisce un'eccezione, dicendo che il comma 1 non viene applicato agli strumenti utilizzati dal lavoratore per rendere la prestazione lavorativa e agli strumenti di registrazione accessi/presenze.

Prendiamo l'esempio (meno attuale) del contatore installato sulle macchine da scrivere per vedere il numero di battute oppure (ben più attuale) l'installazione dello strumento GPS su chi consegna pizze/riders o altro. Che cosa si applica tra il comma 1 o il comma 2 e cosa non si applica?

Risposta: qui non si applica un divieto sul controllo, dunque è ammessa l'installazione, perché se non si applica il comma 1, viene effettivamente (con la nuova norma) installato un dispositivo per tali finalità. L'idea era di evitare di passare dalle associazioni sindacali per l'uso di strumenti per attività lavorative; in questo modo, però, saltano tutti i requisiti funzionali. Deve essere quindi facilmente dimostrato che un certo strumento viene installato per scopi utili alla prestazione lavorativa.

Il nuovo comma 2 pone esclusione sugli strumenti usati dal lavoratore per rendere la prestazione lavorativa e strumenti di registrazione accessi/presenze. Anche qui quindi: l'esonero copre solo gli strumenti rispetto alle normali funzionalità oppure anche nel caso di strumenti finalizzati al controllo personale del lavoratore?

Prendendo l'ordinamento italiano si discute l'utilità delle informazioni raccolte in base ai commi 1/2, si ritengono utilizzabili a *tutti i fini connessi al rapporto di lavoro, a condizione* che sia adeguata 'informazione delle modalità d'uso/controllo e nel rispetto del d. lgs. 30 giugno 2003 n. 196 (esso specifica il significato di "trattamento" come insieme di operazioni che raccolgono dati, visti come "sensibili", "giudiziari" dal "titolare"/"responsabile" degli stessi, ecc.

Maggiori al link: <https://web.camera.it/parlam/leggi/deleghe/Testi/03196dl.htm>

Ci si deve dotare di un "disciplinare interno" redatto in modo chiaro e accessibile da tutti (art. 7 St. lav.), ritenendo corretto l'utilizzo solo al fine utile e al benessere delle "regole del vivere comune" (sentenza cassazione del 2017).

I fini del rapporto di lavoro sono, oltre ai fini disciplinari, anche fini produttivi (premi di produzione, valutazioni performance o, caso pessimo, il licenziamento del lavoratore).

Il lavoratore deve essere informato per certo in merito al tipo di controllo a cui è sottoposto.

Come detto in precedenza, occorre dotarsi di una figura disciplinare interna che faccia redazione in modo chiaro e senza formule generiche, l'affissione dei regolamenti in luogo accessibile, sempre per lo stesso scopo (non vada contro al vivere comune, riforma dell'articolo 4).

A questo sono sottoposte alcune *sanzioni*, per esempio quelle *penali* (da alcune centinaia/migliaia di euro o nel penale reclusione per X giorni), *condotta antisindacale* (giudicando un comportamento inadeguato e usando figure come un giudice del lavoro) o messa in giudizio di dati raccolti ma inutilizzabili. Qualora vi sia un sospetto, il controllo difensivo deve essere proporzionato e pertinente.

I controlli difensivi devono:

- 1) essere diretti ad *accertare condotte illecite* del lavoratore a *tutela di beni estranei al rapporto di lavoro*;
- 2) devono consistere in una verifica effettuata *a posteriori*
- 3) i *risultati* del controllo difensivo possono essere utilizzati *soltanto in modo proporzionato e pertinente* rispetto alla natura stessa del controllo effettuato.

Privacy (inizio parte Ruggiu)

Il confronto al di fuori del nostro ordinamento giuridico è basata sul GDPR (in vigore dal 2016), interagendo con norme già presenti nel nostro ordinamento. Vogliamo quindi capire che il regolamento ai dati personali è un esempio di governance strutturato in maniera “*right based*”, basato sulla protezione dei diritti pubblici/privati, strutturando in modo simile strumenti attuali come quello dell’IA.

Il regolamento si pone come mezzo di:

- tutela delle persone con riguardo al trattamento dei dati
- diritto alla circolazione dei dati

Si tratta in generale di diritti non assoluti, nel senso che il diritto alla protezione dei dati (che è strumentale alla tutela delle persone) deve sopportare affievolimenti (rischi consentiti) e il diritto alla circolazione dei dati deve sopportare alcune condizioni, anche onerose; più in generale, il processo di elaborazione dei dati deve essere utile a servire scopi comuni, a scopo collaborativo.

In particolare, la privacy non è una merce di scambio. Poiché gli scambi commerciali utilizzano sempre più i flussi di dati personali, la riservatezza e la sicurezza di tali dati è diventata un fattore essenziale della fiducia dei consumatori (soprattutto in momenti come oggi con i *big data analytics*, dando attenzione a connotazioni sociali raggruppate, al fine di studiare e analizzare interamente le caratteristiche).

La collaborazione di tutti si inserisce in un quadro più ampio definito come “*governance*”, presenti in vari tipi. Il modello affermatosi in Europa è quella dello *Responsible, Research and Innovation*. In generale con essa si intende la risoluzione di problemi comunitari.

La governance si attua con processi di democrazia attiva e si basa sull’integrazione di due ruoli distinti: quello di indirizzo programmatico (governo) e quello di gestione e fornitura di servizi (strutture operative ed amministrative). Un governo (o government) è strumento di buona governance quando applica principi, mutuati dalla nuova cultura imprenditoriale, per il coinvolgimento e la responsabilizzazione dei cittadini. Il government decide, sotto varie forme di gerarchia, l’applicazione delle direttive di governance, responsabilizzando gli altri soggetti sul successo o meno della tecnologia (sia per le multinazionali che per i privati cittadini). Le decisioni vanno prese prima (*valutazione d’impatto*), prendendo in considerazione le opportune misure (approccio *ex ante*), adempiendo a particolari principi di uniformità (*responsabilizzazione/accountability*).

Si cerca quindi di seguire un approccio che vada verso la new governance, relativizzando l’idea di regolazione e sapendo che ciò che è importante è che i comportamenti sono influenzati dalla modalità applicativa, dipendendo anche da norme morali, sociali o altro. Si ha anche il problema di richiesta del consenso a tutti i soggetti che raccolgono dati personali, dando delle linee di guida di raccolta dei cookies di profilazione/tecnici (*privacy by design*), creando un ecosistema con norme non giuridiche e semplici linee guida/suggerimenti. Il consenso al trattamento dei dati avviene con una serie di obblighi posti da un titolare verso una serie di soggetti interessati, favorendo un meccanismo sanzionatorio in caso di non rispetto.

A questo punto si ha il concetto di *gamification*, introducendo elementi di game design, al fine di rendere agile e semplice nonché accessibile a tutti. La gamification si pone sotto il GDPR, segue RRI (Responsible Research Innovation) e la governance.

La gamification si pone come strumento di aumento di produttività del dipendente, più invogliato e rendendo meglio nella sua attività, oltre che al datore di lavoro, che pone una serie di strumenti tipici del game design (raggiungimento di obiettivi, level-up, interazioni multiutente e una serie di altre cose in grado di poter descrivere questo principio). Essa si pone come ulteriore principio di affermazione ideologica di indipendenza dei lavoratori e dei soggetti interessati, in quanto l’azione stessa di controllo (governing) posta dai soggetti di governo è un modello ormai in crisi, in quanto basato su un unico soggetto e lontano dall’effettiva realtà.

Chiaro quindi come la governance in ambito tecnico-scientifico si ponga come strumento utile di innovazione e di tutela, in un certo senso, dei soggetti terzi e finali interessati, specie se vengono applicate tutele a favore dei soggetti e dei loro dati, dando obblighi al titolare e dando sanzioni pena sorpasso illecito di determinati principi.

Discorso generale sulla privacy e sul ruolo del GDPR

Le istituzioni comunitarie rientrano in gioco, non solo il governo nazionale (es. Authority dati personali), incidendo sull'applicazione delle norme e sull'interpretazione del loro significato.

Ciò si confronta anche con mondi extragiuridici, come ad esempio il mondo etico (norme sociali/morali) ed il mondo politico (linee guida del garante della Privacy), soprattutto in merito all'interazione con il mondo digitale.

Il digitale è ovunque diffuso, partendo dai nostri stessi smartphone, tecnologie wearable, IoT (allarmi, elettrodomestici connessi ad Internet), ecc. La citazione è all'Infosfera, teorizzata da Luciano Floridi, dunque un'interazione totale e quotidiana con i mezzi tecnologici, ormai sempre più entità autonome ed indipendenti.

Discutiamo della *sharing economy*, definito come un sistema economico in cui beni o servizi sono condivisi tra individui privati, gratis o a pagamento, attraverso Internet (ad esempio Uber, Just Eat, Blablacar, ecc.) ed in modalità on-demand, secondo una logica interattiva basata sui singoli (peer-to-peer).

Lo stesso Covid ha portato in primo piano la necessità di informatizzare la vita quotidiana e la nostra stessa interazione, ad esempio nel mondo sanitario o dell'istruzione, sviluppo e gestione centralizzata e digitale. Anche gli stessi vaccini hanno fruito della stessa idea, dato che possono essere considerate fonte di informazione (informazioni genetico-sanitarie).

Il fulcro è la *centralizzazione* riguarda la raccolta dei dati e la loro ricondivisione in tempo reale con altri utenti.

Prendiamo l'esempio di veicoli semi-autonomi; se causano incidenti, esistono normative apposite che si applicano in varie modalità (le norme giuridiche finiscono, ed interviene l'etica, attraverso norme sociali).

Le linee guida possono sfuggire all'applicazione delle norme giuridiche esistenti (ad esempio l'idea di applicazione tramite i cookies), nonché nel quadro politico che cerca di seguire lo sviluppo delle nuove tecnologie (in senso di sviluppo economico, finanziamento di progetti come ad esempio le AI).

La GDPR si pone in mezzo a tutto questo, essendo regolazione dell'UE, ponendo un esempio di come stabilire la governance digitale (privacy, diritto di protezione dei dati, ecc.).

Ad esempio, tramite IoT, diventiamo soggetti capaci di produrre informazione in ogni momento, materiale captabile da una serie di dispositivi, materiale identificante dell'identità della persona. Anche lo stesso diritto all'istruzione si pone come strumento controllato ma in grado di generare disuguaglianze (non disponendo di mezzi tecnologici adeguati, non si può fruire pienamente di questo).

Un altro esempio interessante in questo senso è la tecnologia sintetica, che tramite un insieme di geni cerca di costruire caratteristiche viventi riproducibili, centralizzando ancora di più il controllo uomo-macchina.

Si cita un esempio da parte della filosofa Philippa Foot definito Trolley Problem:

- qui si discutono due casi in cui un treno è fuori controllo e a noi è data la scelta se salvare ben cinque persone facendo deragliare il treno, ma questo investirebbe un solo uomo ammazzandolo, oppure non far nulla, facendo così morire cinque persone.
- Per natura utilitaristica del problema, la maggior parte delle persone salverebbe i cinque uomini, non prendendo quindi in maniera oggettiva, una decisione che salvi l'insieme o di azione del "bene comune"; dunque anche un semplice problema apre vari interrogativi, principalmente per le riflessioni che ne provengono, della duplice natura umana nell'aiuto in senso profittevole.

La stessa regolamentazione dei mezzi autonomi è data dall'articolo 2043 del Codice civile (risarcimento per fatto illecito), riconoscendo personalità giuridica ai robot (titolari di diritti o di obblighi, oppure attraverso forme di assicurazione privata/pubblica); la responsabilità potrebbe ricadere su chi lo ha progettato o sulla stessa macchina (imputabilità giuridica e soggetti coinvolti).

Questo passa attraverso il riconoscimento della personalità giuridica oppure attraverso forme di assicurazione e problemi di policy ponendo il problema di come stia andando la regolazione dell'intelligenza artificiale. C'è poi una questione della disciplina sulla responsabilità dell'omicidio doloso o colposo e la fase di *decision-making* che viene fatto rispetto ai modelli esistenti di governance in un certo settore, nonché l'impatto tecnologico che si può avere (in un campo di regolamentazione nonché di investimenti che vengono fatti, in maniera collegata e dipendente).

Da parte anche delle tecnologie digitali in maniera da preservare alcune finalità che sono riconosciute come prioritarie, quali la protezione dei dati, la ricerca stessa (messa in un ambito generale e come quadro di governance).

Determinati codici etici possono essere sviluppati da privati, evitando sovraregolazioni, tramite ad esempio certificazioni etiche di impresa o patenti da enti certificatori terzi. La regolazione è il tassello che contribuisce al governo di quel settore.

Fondamentalmente si cerca di porre delle regolazioni almeno generali a questioni tecnologiche legate a problemi biologici, in particolare se si dispone di una grande quantità di dati potenzialmente pericolose. Problemi come l'occupazione vengono in parte risolti grazie a regole poste di governance o di soggetti pubblici (stato, UE), ma anche soggetti privati (multinazionali tecnologiche), di dimensioni tali da condizionare la vita dei singoli stati (lobbying), interagendovi in maniera efficace in maniera sovrastatale.

Attraverso un semplice meccanismo "norma e sanziona" non si avrebbero risultati concreti; meccanismi come la UE possono agire in questo senso, grazie alla governance (mondo morale, giuridico, politico) in maniera coordinata e spingendo un settore tramite orientamento verso alcuni risultati (progresso tecnico-scientifico, sviluppo economico, maggiore sostenibilità, ecc.).

La governance si pone obiettivi etici di responsabilizzazione dei soggetti e di anticipazione dei rischi, dato che alcuni comportamenti prevedono sanzioni al fine del rispetto di principi comuni.

I principi etici comuni possono farli coincidere con i diritti (privacy), implementandoli ogni qual volta si ha un trattamento dei dati, affinché essi possano essere affrontati in maniera utile (strumenti giuridici o pareri etici, ad esempio di commissioni scientifiche o di garante della Privacy).

Alcuni modelli si pongono utili per i vari settori, individuando cosa funziona e cosa no in base a ciò che già esiste, capendo in che direzione va il nostro Paese e la stessa UE.

La linea comune di ogni settore è di prevedere anche grazie all'informatica una radicale integrazione con ogni altro settore produttivo, dato che ogni nuova tecnologia può servirsi delle competenze digitali.

Privacy e profili generali regolamento UE

La privacy è considerata *hard law*, in quanto si applica allo stesso modo in tutta l'Unione Europea. Prima del 2016 e il GDPR che è nato in quell'anno, esisteva solo una direttiva che era stata creata nel 1995; in Italia esistevano solo degli atti amministrativi, che non producevano particolari effetti agli stati membri. La direttiva viene recepita normalmente tramite una legge. Vi sono degli ambiti nel regolamento per i quali è lasciato un po' di spazio per i legislatori nazionali per introdurre regole diverse (caso diritto del lavoro). In via definitiva, è entrato in vigore nel 2018.

In questo momento a noi interessa che gli Stati membri possono applicarsi norme specifiche per assicurare la protezione dei diritti in merito al trattamento dei dati ed alle libertà personali. Similmente l'Italia prevede una legislazione più severa in merito alla protezione rispetto ad altri stati esteri, in particolare sui dispositivi e la modalità di controllo. È una norma legittima perché risponde ai criteri dell'articolo, rispondendo ai diritti degli interessati. Grazie al Regolamento, si ha l'omogeneità e l'organizzazione è stata molto più forte. In questo senso si tende a stabilire degli adempimenti sulla base di principi di conformità.

Si capisce dall'articolo 1 del GDPR lo scopo e la finalità di quest'ultimo:

- “1. Il presente regolamento stabilisce norme relative alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché norme relative alla libera circolazione di tali dati.
2. Il presente regolamento protegge i diritti e le libertà fondamentali delle persone fisiche, in particolare il diritto alla protezione dei dati personali.
3. La libera circolazione dei dati personali nell'Unione non può essere limitata né vietata per motivi attinenti alla protezione delle persone fisiche con riguardo al trattamento dei dati personali.”

Il Regolamento non protegge di per sé i dati, ma soltanto gli interessi delle persone fisiche, tutelando i dati riferiti direttamente alle persone fisiche e identificabili. Un ente o un'associazione tratta dati personali che solo in un determinato contesto hanno significato (ad es. la matricola nel campo università, tale che il titolare le possiede e in alcuni casi vengono poi applicate).

I dati devono essere liberi di viaggiare, servendo l'umanità e i suoi scopi.

In questo senso, si evidenzia una grande enfasi in merito agli obblighi dati al titolare e al responsabile, contabilizzando le attività svolte e le misure di sicurezza e di notifica/comunicazione dei dati. Essi non riguardano, come ovvio, un singolo individuo ma interi gruppi sociali, privi di una specifica connotazione ma aggregati sulla base del trattamento *profilato* da algoritmi.

In questo senso, l'articolo 84 del GDPR intraprende, come detto sopra, un approccio *ex ante*, considerando opportune misure che *dimostrano* che il *trattamento dei dati è svolto con rispetto del regolamento* e anche, secondo l'articolo 35, con una *corretta valutazione di impatto* nell'interesse legittimo del titolare e valutando necessità, responsabilità, rischi. La *responsabilizzazione* tende a non definire adempimenti specifici ma definisce principi di conformità, implementando una serie di processi per raggiungere i propri obiettivi.

La privacy non è una merce di scambio, soprattutto oggi dove la digitalizzazione e le frontiere non esistono e ogni settore elabora grandi flussi di dati e/o informazioni.



L'effetto del legislatore si applica indipendentemente dal territorio, secondo l'articolo 3 del GDPR:

"Ambito di applicazione territoriale

1. Il presente regolamento si applica al trattamento dei dati personali effettuato nell'ambito delle attività di uno stabilimento da parte di un titolare del trattamento o di un responsabile del trattamento nell'Unione, indipendentemente dal fatto che il trattamento sia effettuato o meno nell'Unione.
2. Il presente regolamento si applica al trattamento dei dati personali di interessati che si trovano nell'Unione, effettuato da un titolare del trattamento o da un responsabile del trattamento che non è stabilito nell'Unione, quando le attività di trattamento riguardano:
 - a) l'offerta di beni o la prestazione di servizi ai suddetti interessati nell'Unione, indipendentemente dall'obbligatorietà di un pagamento dell'interessato; oppure
 - b) il monitoraggio del loro comportamento nella misura in cui tale comportamento ha luogo all'interno dell'Unione."

Normalmente si possono inviare anche dati all'estero (cosa che per regolamento interno delle aziende spesso accade), ma nel qual caso si applica l'articolo 46 del GDPR:

"Trasferimento soggetto a garanzie adeguate

1. In mancanza di una decisione ai sensi dell'articolo 45, paragrafo 3, il titolare del trattamento o il responsabile del trattamento può trasferire dati personali verso un paese terzo o un'organizzazione internazionale solo se ha fornito garanzie adeguate e a condizione che gli interessati dispongano di diritti azionabili e mezzi di ricorso effettivi."

Il Regolamento si applica solo al trattamento di persone fisiche o anche ai trattamenti parzialmente automatizzati e non automatizzati; non si applica per autorità di pubblica sicurezza o per persone fisiche nell'esercizio di attività di scopo domestico/personale e per attività che non rientrano nell'ambito di applicazione UE.

Si cita in questo senso l'articolo 4 del GDPR (qui citato solo per dare chiarezza dei concetti fondamentali legati al concetto di dato e di suo trattamento):

- 1) «dato personale»: qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale;

2) «trattamento»: qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione;

Dall'articolo 10 del Regolamento, vengono definiti i dati personali relativi a condanne penali e connessi a misure di sicurezza.

Permangono definizioni ad hoc di *dati genetici* (relativi a caratteristiche genetiche ereditarie e che danno informazioni univoche sulla salute mentale, fisica e biologica della persona in questione) e *dati biometrici*, (ottenuti da un trattamento tecnico specifico relativo a caratteristiche fisiche, fisiologiche e comportamentali della persona fisica che ne garantiscono l'identificazione univoca).

Non esiste più una specifica definizione di informazioni sensibili, ma vengono solo individuate categorie di *dati personali* (nel senso di informazioni che rivelano le convinzioni etniche, politiche, sociali, religione dell'individuo e *dati relativi alla salute*, sia essa mentale e fisica.

Altri concetti rilevanti sono:

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

2) «pseudonimizzazione»: il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile;”

Il responsabile del trattamento deve essere in grado di provare sempre la liceità, correttezza, trasparenza, limitazione di finalità, esattezza dei dati e loro integrità/riservatezza e, a tale fine deve dotarsi di una struttura organizzativa adatta a rispondere con flessibilità alle specifiche richieste dei dati che lo riguardano. Le figure chiave della privacy restano il titolare, che determina le finalità ed i mezzi di trattamento dei dati personali, il responsabile, che li tratta per conto del titolare ed il terzo, persona fisica o giuridica che non sia interessato al trattamento e le persone autorizzate sotto l'autorità diretta del titolare.

L'articolo 2 del Codice Privacy prevede proprio delle persone espressamente designate all'interno del proprio assetto organizzativo atte a garantire questo tipo di controllo. In questo senso, ad esempio emerge il DPO (Data Protection Officer), responsabile della privacy. Esso viene designato automaticamente in casi di trattamenti di dati che riguardano il monitoraggio regolare e sistemati di interessati su larga scala, in caso effettuato da autorità/organismi pubblici o quando si parli di condanne penali/reati; in altri casi la nomina è facoltativa. Il titolare dovrà sempre inserire i dati di contatto del DPO, la specifica dei legittimi interessi da lui perseguiti, il periodo di conservazione e il diritto di portabilità, nonché il diritto alla portabilità del dato, di revoca del consenso e di proposta del reclamo.

Similmente, si contratta anche l'eventuale esistenza di un processo decisionale automatizzato, la fonte di origine dei dati personali e le categorie oggetto di trattamento, in combinazione con icone standardizzate eventualmente per fornire un quadro d'insieme del trattamento previsto in modo chiaro (leggibili da qualunque dispositivo).

Il regolamento fonda il proprio consenso dell'interessato sulla base della liceità (articoli 6/7 GDPR), affermando il *consenso* come manifestazione libera ed inequivocabile di assenso e il diritto sempre alla revoca, tale che questa non pregiudichi la liceità dello stesso. Si ha anche il diritto all'oblio, cancellazione dei dati se non sussiste altro fondamento giuridico per il trattamento. L'esecuzione di un contratto o la prestazione di un servizio non possono essere condizionati da un trattamento non necessario. Oltre a questo, non si può precedere ad un trattamento che ha liceità, profilando e trasferendo dati all'estero.

Il titolare e il responsabile del trattamento mettono in atto misure tecnico/organizzative adeguate a garantire un livello di sicurezza commisurato al rischio, che comprendono:

- ✓ La pseudonimizzazione e la cifratura dei dati personali
- ✓ La capacità di assicurare su base permanente la riservatezza, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento
- ✓ La capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico
- ✓ Una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento

L'articolo 32 del regolamento, comma 1, cita quanto segue:

“Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, il titolare del trattamento e il responsabile del trattamento mettono in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, che comprendono, tra le altre, se del caso:

- la pseudonimizzazione e la cifratura dei dati personali
- la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento
- la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico
- una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento”

Non esiste quindi un approccio totalmente responsabilizzante in merito alle misure tecniche e di sicurezza. In merito all'obbligo di documentazione delle misure di sicurezza, è d'obbligo la *redazione del registro delle attività di trattamento*, affrontando rischi e misure tenendo conto di diritti ed interessi legittimi degli utenti interessati.

Il diritto deve essere protetto parallelamente allo sviluppo di un certo sistema di trattamento dei dati:

- *privacy by design*, il titolare del trattamento (tenendo conto dello stato dell'arte e dei costi di attuazione) deve applicare misure tecniche e organizzative adeguate (es. anonimizzazione) volte ad attuare in modo efficace i principi di protezione dei dati e a integrare nel trattamento le necessarie garanzie per tutelare i diritti degli interessati. Tale adempimento va effettuato sia al momento di determinare i mezzi del trattamento (es. progettazione di device) sia all'atto del trattamento stesso;
- *privacy by default*, il titolare deve mettere in atto misure tecniche e organizzative adeguate a garantire che siano trattati, per impostazione predefinita (by default), solo i dati personali necessari per ogni specifica finalità del trattamento. Il titolare può ottenere una certificazione ad hoc, prevista dal Regolamento in base ad una specifica procedura, per dimostrare la conformità ai principi di *privacy by design* e *by default* (artt. 42-43).

Si ha anche la responsabilità civile, intesa come “chiunque subisca un danno materiale o immateriale causato da una violazione del presente regolamento ha il diritto di ottenere il risarcimento del danno dal titolare del trattamento o dal responsabile del trattamento” (art. 82). Il titolare o il responsabile del trattamento è esonerato dalla responsabilità se dimostra che l’evento dannoso non gli è in alcun modo imputabile.

Esistono inoltre sanzioni amministrative pecuniarie, fino a 10.000.000/fino al 2% o fino a 20.000.000/fino al 4% del fatturato mondiale annuo per violazione di obblighi imposti e/o rilevanti del Regolamento nel primo caso e di obblighi rilevati nel secondo caso; per sanzioni penali, la UE non ha competenza, ma è compito degli Stati Membri.

Questioni etiche, giuridiche e politiche delle tecnologie digitali

Si ritorna a discutere dell’imputabilità del danno, in particolare distinguendo tra danno doloso/colposo, obbligando colui che lo ha commesso al risarcimento. I veicoli a guida autonoma rappresentano un primo esempio di norme concernente il nuovo settore tecnologico e la robotica in particolare, riferendoci alla risoluzione di una particolare sentenza del febbraio 2017 (recante raccomandazioni alla Commissione concernenti norme di diritto civile sulla robotica).

Successivamente si è introdotta una proposta di regolamento sull’Intelligenza Artificiale, passata alla Commissione europea 2021, ponendosi come meccanismo di controllo sovrastatale, in cui la regolazione dei singoli Stati viene erosa a favore di una sovranità di organi di massima e comunitari per imporre “dall’alto” una normativa unica.

Già dal ‘700 (Rivoluzione Francese in particolare) lo Stato moderno, inteso come unità singola ed utile a difesa dei valori e dei diritti del popolo visto come singola unità territoriale, decade socialmente e così il diritto (consuetudini, vecchio diritto romano, ecc.) che viene gradualmente sostituito dal monopolio del statale (prendiamo proprio il caso di classi quali nobili/clero che vedono decadere i propri privilegi a favore di queste situazioni).

La regolazione è una perfetta espressione della sovranità di uno Stato, inteso come unità di territorio, popolo e diritto, legittimandone la costituzione in nome del rapporto collaborativo tra cittadini e regolamentazione. Similmente al giorno d’oggi, norme esistenti da molto tempo o anche leggi preesistenti (Codice civile, ma anche Costituzione del 1945 ecc.) vengono gradualmente sostituite da altre regolamentazioni, spesso di natura internazionale (diritti umani, comunità europea, norme UE, ecc.).

Le nuove forme di regolazione concorrenti fanno parte di una visione più ampia, che struttura gli stessi organi in varie categorie (franchising, leasing, globalizzazione stessa), spesso più rapide delle forme di controllo tradizionali. Lo Stato viene quindi sempre più inteso come unità periferica, di ragionamento e crocevia di varie regolamentazioni concorrenti ed accordi tra le singole parti.

A partire dal secondo conflitto mondiale ed avanti, gli Stati sempre più sono intesi come enti che esercitano in maniera esclusiva ed effettiva il governo in una comunità territoriale, normati comunque a livello più alto da organi nel tempo succedutisi; caso particolare in questo senso l’ONU, o anche OMS, quindi organi con conclamato potere organizzativo, di gruppo e di tutela internazionale in ambiti sanitari, di diritti umani, in merito alle minoranze ed i singoli individui, spesso di azione non governativa.

Spesso però, tali soggetti servono o per controbilanciare l’azione di alcuni di questi che tradizionalmente sfuggono al controllo della regolazione oppure si ha una regolazione tale da cercare di imporre obblighi o rispetto di alcune modalità di trattamento e conservazione dei dati (anche privati, come le multinazionali o i big del Web). Lo stesso sviluppo tecnoscientifico, come detto ampliato dagli stessi Stati in un’ottica ampia, è un libero mercato che richiama soggetti di varia natura e, come tali, ciascuno di questi può potenzialmente diventare un *player* decisivo per influenzare la regolazione.

Normalmente soggetti ed attori a livello globale comportano una frammentazione del potere, che spesso si rivela inadeguato alla regolamentazione tradizionale e deve cercare di adattarsi alla complessità crescente della tecnologia.

In questo ambito, distinguiamo un concetto da noi toccato nell'ambito del diritto d'autore come l'invenzione, che richiede conoscenze e strumenti adeguati all'interno del processo produttivo, nonché l'innovazione, processo che muove e porta invenzioni ad un miglioramento, a scopi di bene sociale ed economico o per acquisire un vantaggio sui competitor, accelerando l'innovazione stessa.

Se da un lato le tecnologie sono un bene per i motivi citati di innovazione tecnologica, dall'altro si hanno rischi etici, scientifici e sociali oltre che giuridici di tutte le parti in gioco.

Come detto, a parte la ICT, anche settori come le bio/nano tecnologie sono in continua espansione, sia nello stesso Occidente che cerca di rimanere al passo, sia in paesi di sviluppo, uniformandosi ad una linea comune che coinvolge prodotti/servizi/stili di vita delle stesse popolazioni.

Il fenomeno che coinvolge spazio e tempo si irradia in un progetto a luce comune negli USA o in Europa, che porta sempre più alla delocalizzazione di impianti principali, ma anche l'ubiquità, sia in ambito fisico che in ambito Web. Il mondo globale interconnesso, dunque, attraversa certamente un rischio legato sia ai cambiamenti ambientali (pandemia), terroristici (eventi vari degli ultimi anni) ed economici (crisi EU, Grecia, delocalizzazione ed ubiquità delle aziende), con vantaggi ma anche rischi che tendono a distribuirsi, venendo meno le responsabilità dei singoli.

Le tecnologie, dunque, possono convergere per fare nuovi prodotti o servizi o essere abilitanti, dando vita a nuovi settori disciplinari (nanomedicina, biologia sintetica, ecc.), trovando nuove soluzioni a problemi esistenti. Quindi la scienza passa dall'essere *technology-driven* ad essere *problem-oriented*, orientandosi a soluzioni di terze parti e spesso collaborative.

A questo si discute se il diritto sia effettivamente obsoleto, ma la stessa gente deve poter decidere cosa vuole e come (*public engagement*), creando strumenti flessibili e adattabili al contesto tali da garantire le preferenze delle persone in un determinato momento storico. Dunque, se la regolazione non è più l'unico strumento in grado governare i fenomeni, si parla di *governing*, inteso come una pluralità di forze con capacità di governo che agiscono insieme sfuggendo alla regolazione tradizionale, lenta ed inefficace.

Si parla quindi di una *meta-governance*, tale quindi da far entrare questa risoluzione comunitaria nei vari ambiti (sintesi di governance, insomma), con strumenti e processi (formalizzati e non), garantiti da soggetti singoli e atti di soft/hard law, linee guida, report ufficiali e varie forme di regolazione. Il fine ultimo è sempre il progresso comunitario, idealmente.

La governance viene vista come un insieme di soggetti e strutture orientate al benessere economico ed al progresso tecnoscientifico in modalità sostenibile e distribuita; il modello di potere si basa su un soggetto dominante, sensibilizzando la pluralità di soggetti coinvolti e idealmente costruendo insieme. Se gli attori sono distribuiti, possono sfuggire alla regolazione; dunque, fondamentale introdurre un approccio top down, fatto di linee guida, regolazioni comportamentali, codici etici che possono permeare la società e, potenzialmente, tradursi poi in forme di "hard law".

Teoria e modelli di governance

Grazie alle tecnologie emergenti ed una globalizzazione diffusa a livello modulare, la regolamentazione non è più singolarmente in grado di disciplinare la condotta e per spingere i consociati a seguirla si pone una sanzione. I diritti fondamentali sono protetti a livello internazionale e nazionale in maniera biunivoca.

La *governance* viene definita come:

“l’insieme di processi a carattere reticolare e diffuso tra i diversi attori pubblici e privati a livello nazionale e sovranazionale, costituiti da norme giuridiche hard e soft, tra loro variamente coordinate, per risolvere conflitti e adottare decisioni in un particolare settore (tecnologico, economico, finanziario etc.)”.

La teoria della *governance* nasce nell’ambito della business ethics al fine di studiare i principi e i meccanismi della gestione d’impresa. Al di fuori dell’ambito dell’impresa:

- studia la *governance* :
 - o origine del concetto, caratteristiche, struttura, e finalità
- elabora modelli di *governance*
 - o le tipologie di *governance* che possono essere realizzate e quali tipologie sarebbe opportuno realizzare

La questione dei dati personali rappresenta una forma di disciplina regolata da norme e concetti compresi da regolazioni o consuetudini, sfuggendo al campo del diritto.

Il concetto di *governance* è più flessibile e segue il percorso dell’innovazione tecnologica, aggiornandosi e imparando dai propri errori, dando problemi di occupazione e regolamentazione.

Possiamo quindi fotografarla e capire quali modelli si stanno attuando.

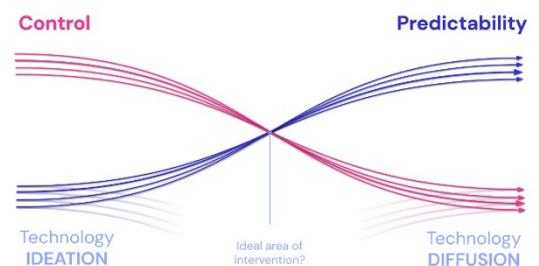
Tra questi, in particolare, abbiamo l’idea di *new governance*, caratterizzato da particolare resilienza e flessibilità, coinvolgendo in maniera distribuita i diversi attori in gioco. Il concetto nasce in particolare nella UE per i problemi legati all’occupazione ed all’ambiente.

In ultimo, i soggetti si pongono dubbi in merito alle loro responsabilità e doveri, sviluppando in autonomia modelli attenti ai diritti e che portano a comprendere la responsabilità delle proprie azioni.

Nelle prime fasi, il processo di innovazione implica dilemmi sociologici, quali il *dilemma di Collingridge*, che riassume il fatto che la tecnologia non riesce a stare dietro al controllo posto sulle stesse informazioni.

Nel momento in cui una tecnologia inizia ad esistere, siamo in grado di intervenire tramite strumenti regolatori ma non abbiamo sufficienti informazioni per regolarlo. Dunque, o si interviene subito castrando l’innovazione oppure si interviene troppo tardi.

Graficamente è come a lato.



Adapted from Bessis, F. & Samoni, F. (2008) Responsibility driven design for the future self-driving society. Fondazione Giannino Bassetti.

Nell’ambito sociologico, si sono sviluppati studi interdisciplinari, che cercano di avviare una discussione interdisciplinare sul rischio e sull’approccio all’innovazione, discutendone insieme.

Le principali osservazioni poste sono:

- la democratizzazione dell’etica, prima ridotta a sole élite scientifiche
- la democratizzazione della *governance*, non più solo in mano a pochi soggetti pubblici

Attorno al dibattito sulla governance, si cerca di valutare l'impatto delle tecnologie emergenti, sotto controllo etico, giuridico e sociologico e ponendo pubbliche discussioni (*public fora*), con stakeholders distribuiti su scala globale. Gli strumenti cercano di creare una governance distribuita, usando schemi flessibili e non rigidi, sensibili al contesto applicativo e culturale.

Prendiamo l'ambito della geoingegneria, sottoposta al coinvolgimento continuo di organi collaborativi e società civile per cercare di risolvere i problemi legati al cambiamento climatico, giungendo attraverso una serie di fasi alla creazione di un progetto a livelli nazionali.

Essendo problemi complessi, si cerca di adottare un insieme di soluzioni uniformi in maniera flessibile e procedurale secondo una serie di obiettivi posti a livello dei singoli stati, sia in senso di sperimentazione ma anche di decentralizzazione degli approcci esistenti; tutti per uno ed uno per tutti, banalmente.

La new governance si pone come modello informale, tale da garantire regolazione tramite strumenti giuridici ed atipici, non accompagnati da strumenti sanzionatori, con strumenti di soft-law (linee guida, suggerimenti sul come comportarsi). Il modello è *eterarchico*, in cui la legge non è intesa come modello classico di regolazione (un solo regolatore dall'alto), ma prende atto che i soggetti sono molteplici e possano sfuggire a regolazioni singole.

Il regolatore può comunque disciplinare ogni condotta secondo un modello *command-and-control*, senza la regolamentazione dall'alto. Il *public engagement* si propone di coinvolgere le parti unilateralmente a prescindere dal loro livello di influenza, pur essendo consapevole che determinate persone ed organi inficino anche pesantemente a livello globale (es. Zuckerberg, fondatore di Meta, potenzialmente ha più potere di molti altri stati e può sedersi assieme a loro discutendo dei problemi globali).

Si pone anche un'idea di autodisciplina dei singoli settori, estendendo una forma di controllo anche a livelli esterni/più generali, portando a vantaggi estesi.

Nell'ambito quindi della strategia di lavoro, si ha un principio di obiettivo comune, facendo in modo che tutti gli Stati scelgano in modo libero e decentralizzato, gli approcci da adottare, sperimentando diverse soluzioni in modo flessibile. L'idea della new governance è la "wait and see", dunque attendere che la situazione si evolva prima di adottare una regolazione predefinita, come accennato prima.

Nel quadro della *new governance*, la governance assume un carattere sperimentale, assumendo caso per caso un carattere di apprendimento sugli errori del passato. All'interno di conferenze, in particolare, si individuano pratiche generali e alcune regolamentazioni vanno verso l'idea di autonomia, nel riscontro della *self-governance*, soprattutto in settori come quello tecnologico, per cui tutti i soggetti sono sullo stesso piano e cercano di auto-organizzarsi, dandosi poche regole spontanee anticipando il pubblico.

È ad esempio il caso della biologia sintetica, caso in cui nella prima decade del 2000, si sono discusse le best practices atte a favorire il dibattito internazionale e porre un'idea di autenticità e sicurezza dei dati raccolti. Si cerca inoltre di creare e disegnare modelli di risoluzione di problemi (cosiddetto *codesign*, secondo un modello fai-date/DIY) per soluzioni a problemi comuni e verso gli utenti: esempio *Nightscout Project*, sottoposti ad un monitoraggio continuo del glucosio, quindi problemi legati al diabete.

In ultimo, la ricerca deve essere rispettosa dei soggetti interessati, da un punto di vista etico, prima di tutto, analizzando rischi e responsabilizzando le parti in gioco, in un quadro di accettabilità (strumenti come questo sono un potenziale rischio alla privacy, eventualmente correggendo approcci di governance).

Similmente, parliamo di *tentative governance*, intesa come studio delle tecnologie emergenti e relativi schemi applicativi, ragionando caso per caso ed imparando dagli errori del passato (*governance case by case*). In ambito tecnico scientifico, quindi, sono nati dei codici di condotta tra i vari gruppi industriali, regolanti la crescita e l'andamento dell'innovazione. L'obiettivo è favorire lo sviluppo secondo un dibattito condiviso tra gli stakeholders (multi-stakeholder), costituendo dei working group.

Responsible Research Innovation (RRI)

La Responsible Research and Innovation/RRI nasce nell'ambito europeo come modello di governance per poter affrontare rischi legati alla ricerca ed all'innovazione, in maniera eticamente accettabile. Elaborato a livello accademico, si pone come applicazione della new governance. Ha alcune caratteristiche:

- 1) carattere *anticipatorio*, identificando tempestivamente rischi
- 2) carattere *partecipativo*, con coinvolgimento degli stakeholders (public engagement)
- 3) *considerazione anche della perdita di opportunità*, non solo incentrati sul rischio
- 4) *accettabilità etica e desiderabilità sociale*, con valori etici condivisi e considerazione dei bisogni della società civile

Dall'interazione dei vari elementi si vuole creare un quadro generale caratterizzato da ricettività (*responsiveness*), recependo gli input dal basso con bisogni e valori della società civile e riflessività (*reflexivity*), riflettere su quali scopi si debba perseguire l'innovazione, mettendo al centro una serie di valori. Da una parte recettivamente assorbiamo i bisogni della società civile e dall'altra si cerca di costruire tramite una serie di valori, un meccanismo di innovazione responsabile (all'interno del mondo accademico ad esempio). Il modello della RRI è adottato a livello comunitario in tutta l'UE (ad esempio programmi come Settimo Programma Quadro per l'innovazione, finanziamento della UE per l'innovazione).

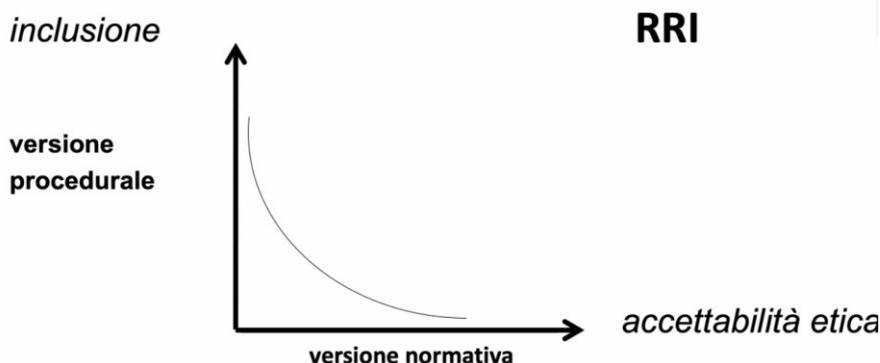
Nonostante l'unanimità del mondo accademico, esiste divergenza sulla definizione e sulle finalità, avendo un disaccordo etico di fondo sui valori della ricerca e dell'innovazione.

Si identificano due tendenze, non schieramenti opposti ma due possibilità all'interno dello stesso modello:

- un approccio procedurale
- un approccio normativo-sostanziale

Si concorda sulla centralità dell'inclusione basandosi sui valori condivisi, sia in merito a come devono essere configurati essi stessi o la configurazione stessa dei processi di public engagement.

Idea grafica tra versione procedurale (spingiamo su quella tramite il public engagement) e normativa:



La concezione procedurale ritiene fondamentale il processo di identificazione dei "valori condivisi", a cui appartiene l'innovazione, cercando di capire quali valori di natura sociale mantenere ("anchor points").

La regolazione risulta essere antiquata, focalizzata sulle condotte passate che non possono essere riprodotte con l'innovazione. Si ha quindi un "gap della responsabilità", in quanto nessuno può essere ritenuto responsabile in circostanze conoscibili/imprevedibili; il legislatore quindi può non essere organizzato (si parla di "irresponsabilità organizzata").

Le condotte passate non sono quindi in grado di comprendere le nuove situazioni, spinto dalle tecnologie emergenti; similmente, il concetto di sanzione (*liability*) segue questo principio *ex ante*, ragionando in precedenza. La responsabilità statale, nonostante si trovi in situazione di non regolazione, si assume le responsabilità etiche della propria azione.

Gli stakeholders, dunque, vengono progressivamente coinvolti, attraverso procedure aperte, inclusive e democratiche, variando da contesto a contesto. Si vuole colmare un deficit di legittimità delle istituzioni, tale da identificare i valori condivisi dell'innovazione; i valori cambiano nei vari contesti culturali e tecnologici, preservando la procedura. La governance è costruita in termini sperimentali, ragionando *case by case* sui singoli casi di innovazione per capire come sia avvenuto il public engagement, nel nome della libertà della ricerca e dell'innovazione (*Responsible Innovation*).

Affinché l'innovazione recepisca i bisogni della società, si ha bisogno di meccanismi che coinvolgano i bisogni e le priorità. La procedura ha lo scopo di portare la società civile a riflettere in merito ai propri valori etici ed alle priorità, dando una visione di futuro in maniera ricettiva (*vision*) e riflessiva la società civile alla conoscenza dell'innovazione (caso citato per fasi della geoegegneria, citando l'esempio di costruzione di quadro aperto e democratico della società inglese era la SPICE (Social cohesion, Participation, and Inclusion through Cultural Engagement), rendendo la gente consapevole dei cambiamenti del clima e dell'intervento della geoegegneria, peer poter far calare la temperatura nel caso della Gran Bretagna).

La *vision* è un processo collettivo, che indica la direzione dell'innovazione, spesso data da personalità nuove e visionarie, quali Steve Jobs o Elon Musk. Alla fine di questo percorso, si giunge ad una visione non più appartenente ad un singolo soggetto ma all'intera società civile.

Non ci devono essere rischi per l'ambiente e si deve rispettare la legislazione vigente; dato questi valori si deve coinvolgere la società civile e indicando le future applicazioni nella geoegegneria.

Si hanno dei punti di ancoraggio normativo "*normative anchor points*", valori delle costituzioni e dei trattati, ritenendo che ricerca ed innovazione debbano aprirsi alla partecipazione degli stakeholders, secondo dei valori di accettabilità etica. Ci sono casi di fallimento dell'innovazione, ad esempio gli OGM, causati dalla mancanza di adeguata informazione e partecipazione.

Per risolvere le questioni di divergenza in merito ai valori, si deve fare riferimento ai diritti fondamentali garantiti dalla direzione comunitaria della UE, oppure a livello nazionale in merito alla Costituzione. Ora, questi valori funzionano come filtri, quali progetti finanziare al fine di ottenere uno sviluppo sostenibile e competitivo, al fine di preservare anche la dignità umana e il progresso.

I normative anchor points comprendono quindi anche i diritti fondamentali; dunque questo modello RRI è un modello *right-based*, incentrato sulla protezione dei diritti (studio e manipolazione di nuove tecnologie, in merito anche ad un discorso etico e di condotta, ad esempio le nanotecnologie).

La collaborazione richiede una partecipazione discussa ed attiva, individuando quindi valori e principi etici.

Non tutti concordano sugli stessi valori, essendo spesso ambigui e conflittuali; i fini della UE sono bilanciabili e possono essere sacrificati in tutto o in parte per determinati obiettivi comunitari.

Importanti sono i valori, ma anche la collaborazione bilanciata, ad esempio la BRICS (comprendente Brasile, Russia, India, Cina, Sudafrica), con valori ambigui e conflittuali.

Generalmente, si ha un rischio di *litigation* tra i diritti fondamentali già garantiti dentro la UE e non bilanciabili con altri interessi pubblici dello stato, rischiando di far venir meno il principio dell'innovazione e di ricerca, soprattutto in merito alla prevalenza dei diritti giudiziari. Il mancato rispetto dei diritti può portare a cause che vanno in contraddizione con la versione procedurale di protezione (diritti umani) oppure sul bilanciamento di obiettivi ed obblighi (implementando i diritti della governance, versione normativa), secondo un'etica dei diritti utilitarista.

In Europa ci sono due sistemi di protezione dei diritti: quello dell'Ue con la Corte di giustizia e quello del Consiglio d'Europa con la Convenzione europea dei diritti dell'uomo e la Corte di Strasburgo e i diritti fondamentali/umani non coincidono del tutto; infatti, si deve tenere conto dei vari limiti presenti.

Il regolamento generale protezione dati personali/GDPR

L'idea di privacy è il diritto alla riservatezza, quindi uno spazio riservato in cui il soggetto ha controllo, autonomia e diritto alla protezione dei dati che lo riguardano.

Le norme che la proteggono principalmente sono la Convenzione Europea dei Diritti dell'Uomo (CEDU) del 1950 art. 8 (Rispetto della vita privata e familiare) e la Convenzione sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale n. 108 del 198; all'interno della UE abbiamo: Trattato di Maastricht 1992, che culmina il processo di integrazione del mercato unico e la Direttiva 46 del 1995 per avere una normativa quadro a livello europeo sulla protezione dei dati .

Gli Stati sono liberi di scegliere i mezzi per implementare gli obiettivi

Discutiamo il caso *Cambridge Analytica* per discutere il caso *privacy by design*, analizzando come di fatto il voto delle persone fosse stato influenzato preferenzialmente verso alcune fonti, attraverso lo studio accurato dei dati personali degli utenti tramite login Facebook.

Lo stesso Comitato europeo per la protezione dei dati si pone come organo indipendente atto a fornire linee guida e regolamento sulle comunicazioni e sul controllo posto agli stessi mezzi di comunicazione.

Le istituzioni esistenti a livello europeo contribuiscono, per mezzo ad esempio del Gruppo di lavoro articolo 29, comprendente tutte le Authority e garanti esistenti a livello nazionale, sostituito poi dall'*European Data Protection Board*, organo europeo che contribuisce parimenti alla protezione dei dati in tutta la UE.

Essa fornisce l'*opinion* (idea) di proposta di regolazione ai dati personali, oppure alle comunicazioni elettroniche e alla vita privata. Il GDPR differenzia in maniera marcata la legislazione esistente in tutto il resto del mondo in merito a questa materia.

Si vogliono quindi eliminare le differenze interne che impediscono la libera circolazione dei dati all'interno del mercato europeo proteggendo i diritti fondamentali dei cittadini europei.

In Italia esisteva già il Codice della privacy ed un sistema *opt-in*, raccogliendo dati solo tramite consenso.

Si distinguono alcuni soggetti:

- 1) Il titolare del trattamento, persona od istituzione che ha le responsabilità del trattamento
- 2) Il responsabile del trattamento, che lo esegue per conto del titolare
- 3) L'interessato, persona od impresa i cui dati sono trattati
- 4) DPO (Data Protection Officer), responsabile della privacy e che entra in gioco in determinate situazioni, soprattutto quando sono raccolti in modo massivo.

Accanto alle diverse tipologie di soggetti, si hanno varie tipologie di dati:

- dato, qualunque informazione (personale o meno)
- dato personale, che riguarda una persona fisica individuata ed individuabile (identificando le idee sindacali, religiose, politiche, biologiche, ecc.), quindi una serie di categorie di dato (art.9,1 e art.10 da parte del Codice della Privacy)
- particolari categorie di dati, in grado di rivelare l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, ecc.

I dati non possono essere trattati senza il consenso dell'individuo, adempiendo all'obbligazione o rispetto del trattamento dell'interessato, protezione di interesse vitale dell'interessato e pubblico dominio del dato. Il trattamento è necessario per il trattamento e la difesa di un diritto nel caso giudiziario o di pubblico interesse nel caso di statistica o di sanità (*dati sensibili*).

Nel caso di informazioni genetiche particolarmente serve il consenso e anche una autorizzazione ad hoc del Garante della privacy. Il dato è personale non per la sua natura, ma per la fonte da cui proviene, anche se apparentemente irrilevante, una volta integrato con altre informazioni utili a identificare un soggetto.

Normalmente è proibita, ma se il trattamento non richiede l'identificazione dell'interessato il responsabile del trattamento non è obbligato a conservare, acquisire, trattare ulteriori informazioni per identificare l'interessato (art. 11).

I principi della *privacy by design* sono:

- 1) liceità, correttezza e trasparenza
- 2) principio della limitazione del trattamento, con finalità note, esplicite e legittime
- 3) principio della minimizzazione dei dati, tali che essi siano pertinenti e necessari alle finalità
- 4) principio dell'esattezza, esatti e possibilmente aggiornati
- 5) principio della limitazione della conservazione, allo stretto necessario
- 6) principio dell'integrità e riservatezza, trattati in modo sicuro

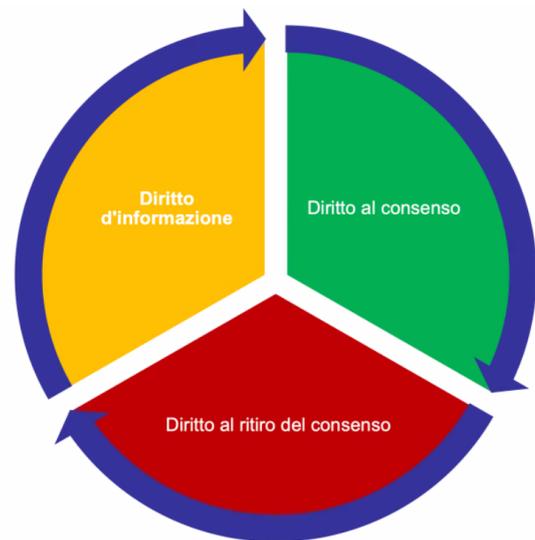
Quando l'interessato ha dato il proprio consenso, firmando un contratto, si deve rispettare un obbligo giuridico, si deve proteggere la vita dell'interessato, compito di interesse pubblico e legittimo interesse del titolare del trattamento, si ha la *liceità del trattamento*.

Il Regolamento è costruito su un nucleo di diritti dell'interessato, ad es. diritto di accesso, rettifica, cancellazione, limitazione al trattamento e portabilità dei dati, nonché l'opposizione alla profilazione.

La *privacy by design* è quindi un accordo di scambio, ad esempio il caso del diritto al consenso al trattamento e ritiro del consenso.

Il titolare deve essere in grado di dimostrare che l'interessato ha consentito in modo chiaro, tale che sia distinguibile da ogni altra materia.

Le informazioni sul trattamento, sul titolare, sulle finalità e durata del trattamento e sulle misure tecniche adottate devono essere scritte in modo leggibile e chiaro in un documento di *soft law* come applicare le norme di *hard law* del GDPR.



Lo stesso consenso al trattamento deve essere *esplicito* (manifestato prima dell'inizio dello stesso), *specifico* (con specifiche finalità), *informato* (dato sulla base di informazioni chiare) e *documentabile* dal titolare del trattamento.

Il titolare deve essere in grado di dimostrare che l'interessato abbia acconsentito, prestato in modo chiaramente distinguibile da ogni altra materia l'acquisizione del consenso; similmente, l'interessato ha il diritto a ritirare il consenso in qualsiasi momento e, generalmente, possiede:

- diritto all'informazione del trattamento, il titolare, le finalità e la durata
- diritto all'oblio, cancellazione dei dati quando non più necessarie e ritiro del consenso
- diritto di accesso dei dati intervenendo sul titolare, confermando che esiste un trattamento riguardante i propri dati personali e avendo informazioni sulla durata e sui destinatari del trattamento
- diritto di rettifica in merito ad inesattezze sui dati
- diritto di limitazione del trattamento, contesta quanto la raccolta sia lecita
- diritto di opposizione al trattamento dei dati o alla sola raccolta automatizzata/AI
- diritto ad un ricorso giurisdizionale effettivo a protezione dei propri diritti e di responsabilità/danni subiti

Corrispondentemente, il responsabile dei dati li tratta e fa le veci del titolare e attua le misure necessarie a dimostrare l'adempimento al Regolamento. In determinate situazioni, il soggetto incaricato dal titolare o dal responsabile di fronte alle autorità del controllo e dell'interessato.

L'interessato deve essere informato:

- sul trattamento che lo riguarda e sui suoi diritti;
- su chi è il titolare responsabile del trattamento;
- su chi è il responsabile del trattamento e, eventualmente, su chi è il 'DPO';
- sulle finalità del trattamento;
- sulla durata del trattamento;
- sull'eventuale esistenza di un trattamento automatizzato;
- sulle misure tecniche adottate per la protezione dei dati (anonimizzazione, pseudonimizzazione, accesso ristretto, firewall, password etc).

La nomina di un DPO è necessaria quando:

- il trattamento è svolto da una pubblica autorità o da un ente pubblico
- la finalità del trattamento dei dati è regolare ed effettuato su larga scala (specie dati sensibili, quali biologici e biometrici)
- il trattamento riguarda particolari categorie di dati (biologiche/genetiche/ecc.)

Si deve tenere un registro di attività del trattamento, quindi nome e dati del titolare, finalità e dati stessi. Preventivamente, deve essere avviata una valutazione dei rischi ed è necessario quando si ha una valutazione estesa e sistematica delle persone fisiche basate su un processo automatizzato.

Tale cosa è definita come *Privacy Impact Assessment*, tale che:



In caso di urgenza, il Garante della Privacy può bloccare la vendita e ordinare che l'interessato sia informato dal titolare e abbia nuove possibilità di prestare il consenso.

In merito all'uso secondario dei dati, si ha una revisione in merito alla questione UI, tale da favorire la diffusione dei dati in maniera accessibile (*open data*), sviluppando il mercato internazionale.

Si vuole quindi garantire la protezione della sicurezza pubblica, con infrastrutture sensibili, proteggendo i dati personali dall'identificazione.

Caso interessante: Tiziana Life Science, studio della ricerca del DNA di una popolazione sarda molto longeva. Per cercare di capire le origini genetiche si è avviata una ricerca tale da consentire anche agli stessi cittadini di verificare l'appartenenza a questi gruppi (*citizen veillance*).

I campioni biologici sono stati poi rubati e poi successivamente ritrovati.

Gamification

Presentiamo la tutela dei diritti personali come strumento che testimonia il passaggio dalla regolazione statale a quella sovrastatale e questo perché il regolamento personale ruota intorno al concetto di privacy by design, quindi i dati devono essere protetti o per impostazione questa vita perché si eliminano una serie di informazioni che non sono funzionali alla finalità di un determinato trattamento, soprattutto se si parla di dati personali, adottando contromisure per evitare che vengano sottratti dati dei privati.

Oggi vedremo un caso di applicazione del GDPR nel tema della *gamification* nell'ambiente di lavoro, vale a dire l'introduzione di elementi presi dai videogiochi in contesti non ludici, come nella sanità, a scuola, in campo militare, della circolazione stradale, nell'ambito del training (chirurgia, aviazione), nell'ambiente di lavoro.

Il suo fine è modificare le motivazioni del lavoratore per indurlo a seguire "spontaneamente" determinate buone pratiche che l'azienda individua come strategiche facendogli apprendere nuove competenze, corrette abitudini lavorative, assumere i ritmi di lavoro più convenienti, seguire speciali forme di training, percorsi di aggiornamento. Idealmente si vorrebbe l'intima e volontaria adesione del dipendente al programma implementato dall'impresa, al fine di renderlo maggiormente coinvolto nella mission e negli obiettivi aziendali. In questo senso, si introducono avatar, forme di cooperazione o competizione tra gli utenti del gioco, sfide, punteggi per il passaggio di livello, speciali classifiche (leaderboards) in cui si possono seguire i risultati raggiunti e gli avanzamenti di livello.

Nel caso di Amazon, si ha avuto un caso di gamification: cinque magazzini con vari giochi all'interno dei vari dipartimenti, in cui il dipendente segue sullo schermo della propria postazione lavorativa la progressione del gioco in cui è impegnato, cioè della mansione che gli è stata affidata. Grazie ai sistemi di tracciamento, i pacchi, tutti tracciati, possono essere seguiti dal sistema che poi ne condivide gli spostamenti sullo schermo della sua postazione come in una sorta di Tetris.

Segue sullo schermo gli avanzamenti dei propri compiti, oppure mostra lo stesso lavoratore o interi reparti in competizione tra loro. Da una parte quindi:

- il lavoratore trae soddisfazione dal raggiungimento degli obiettivi, degli avanzamenti di classifica, dai premi che via via ottiene e si allevia la fatica di compiti ripetitivi, abbassando il livello di stress di mansioni particolarmente impegnative e venendo incontro alle preferenze del lavoratore e alla sua voglia di distrarsi e divertirsi (appassionandosi alla mansione);
- il datore di lavoro ottiene come risultati una migliore organizzazione, maggiore produttività (stimolando il lavoratore nelle mansioni affidate e adottando le prassi corrette di regolamentazione), il miglioramento delle prestazioni professionali, non rinunciando al fattore competitività dell'umano che lo spinge a superarsi inconsciamente.

I game design elements producono un miglioramento delle performance del lavoratore, a livello fisico, psichico, performance temporanee (training) e non temporanee (normali mansioni affidate).

Mansioni ripetute ed estenuanti a livello fisico possono logorare fisicamente parlando, specie se parliamo di mansioni svolte per un tempo indefinito; da questo punto di vista la gamification si pone doppiamente in atto per meglio coinvolgere ed alleviare, sia mentalmente che fisicamente, l'impegno profuso.

I diritti del lavoratore vanno tutelati:

- Diritto alla salute : le condizioni di salute del lavoratore sono ulteriormente sollecitate (viene a fare e desiderare ciò che altrimenti non avrebbe fatto o voluto, quasi soggiogato)
- Auto-determinazione : agendo sulle motivazioni del soggetto che lo spongono a compiere le mansioni
- Privacy: i «game design elements» per funzionare «mangiano dati» dei lavoratori

La gamification agisce sulla motivazione del lavoratore, in quanto il lavoratore non esegue più i compiti assegnategli “perché deve”, ma “perché gli piace”; chiaro dunque il rischio di sviluppo di forme di game addiction, dipendenza e ludopatia.

La creazione di avatar, classifiche, leaderboard banner, meccanismi di competizione all’interno dell’azienda implicano la raccolta, la conservazione e il trattamento di una gran quantità di dati personali dei lavoratori, nonché di localizzazione, registrazione di preferenze, elementi psicoattitudinali, condivisi con il datore di lavoro ed i colleghi. Cresce quindi in maniera esponenziale il controllo esercitato.

Il controllo dei dati è funzionale al controllo della capacità di autodeterminarsi (*empowerment* del soggetto), implementando la privacy del lavoratore by design si rafforzano le condizioni dell’autonomia. I correttivi alla gamification prendono i principi base della RRI, dunque la partecipazione attraverso dibattito ed implementazione privacy e autonomia.