Agenzia nazionale per le nuove tecnologie, l'energia e lo sviluppo economico sostenibile

Ministero della Transizione Ecologica

Ricerca di Sistema elettrico

Comunità energetiche e implicazioni in tema di dati personali. Riflessioni operative per possibili itinerari

Giovanna Iacovone; Giordana Strazza

Report RdS/PTR2021/047

COMUNITÀ ENERGETICHE E IMPLICAZIONI IN TEMA DI DATI PERSONALI. RIFLESSIONI OPERATIVE PER POSSIBILI ITINERARI

Giovanna Iacovone; Giordana Strazza (Università degli Studi della Basilicata)

Dicembre 2021

Report Ricerca di Sistema Elettrico

Accordo di Programma Ministero della Transizione Ecologica - ENEA
Piano Triennale di Realizzazione 2019-2021 – III annualità
Obiettivo: Tecnologie
Progetto: Tecnologie per la penetrazione efficiente del vettore elettrico negli usi finali
Work package: Local Energy District
Linea di attività: LA1.55"Principi, procedure e adempimenti per il trattamento dei dati personali: protezione, sicurezza dei dati e delle informazioni raccolte"
Responsabile del Progetto: Claudia Meloni, ENEA
Responsabile del Work package: Claudia Meloni, ENEA

Il presente documento descrive le attività di ricerca svolte all'interno dell'Accordo di collaborazione "Principi, procedure e adempimenti per il trattamento dei dati personali: protezione, sicurezza dei dati e delle informazioni raccolte"
Responsabile scientifico ENEA: Sabrina Romano
Responsabile scientifico Università degli studi della Basilicata: Giovanna Iacovone
Ringraziamo il Responsabile scientifico ENEA (Sabrina Romano) e gli altri ricercatori dell'Ente (in particolare, la Responsabile del Progetto, Claudia Meloni, e Gilda Massa) per la collaborazione nell'individuazione dei casi di studio per la ricerca.

Indice

SOMMARIO 4
1 INTRODUZIONE 5
2 DESCRIZIONE DELLE ATTIVITÀ SVOLTE E RISULTATI 9
2.1 1° STEP: INDIVIDUARE IL TRATTAMENTO DI DATI PERSONALI 10
2.2 2° STEP: INDIVIDUARE I DATI PERSONALI TRATTATI E SE RIENTRANO IN "PARTICOLARI CATEGORIE" 12
2.3 3° STEP: INDIVIDUARE IL TITOLARE (O I TITOLARI) DEL TRATTAMENTO, IL RESPONSABILE E GLI ALTRI SOGGETTI COINVOLTI 14
2.4 4° STEP: INDIVIDUARE GLI INTERESSATI E GARANTIRE IL RISPETTO DEI LORO DIRITTI 18
2.5 5° STEP: VERIFICARE SE OCCORRE UNA VALUTAZIONE DI IMPATTO 24
2.6 6° STEP: ADOTTARE LE MISURE DI SICUREZZA OPPORTUNE 25
2.7 7° STEP: NOTAZIONI IN CASO DI TRASFERIMENTI DI DATI VERSO STATI TERZI 25
2.8 FOCUS SUL RAPPORTO TRA PRIVACY E NUOVE TECNOLOGIE: LA DATA PROTECTION IN CASO DI SMART METERS, PIATTAFORME, BLOCKCHAIN E SMART CONTRACTS 27
2.9 CASI DI STUDIO 36
2.10 CASO A - DIMOSTRATIVO SPERIMENTALE CON ACQUISIZIONE DATI IN TEMPO REALE 37
2.11 CASO B – UTENTI PIATTAFORMA CHE COMPILANO UN QUESTIONARIO 39
2.12 CASO C – UTENTI DELLA SPERIMENTAZIONE LOCAL TOKEN ECONOMY 40
2.13 CASO D – ADESIONE ALLA COMUNITÀ ENERGETICA 41
2.14 CASO E – PIATTAFORMA SOFTWARE IN GRADO DI MONITORARE I SOCIAL MEDIA WEB PER ESTRARRE INFORMAZIONI SULLE COMUNITÀ ENERGETICHE 42
3 CONCLUSIONI 43
4 ALLEGATI 45
4.1 CHECK LIST E DIAGRAMMA 45
5 RIFERIMENTI BIBLIOGRAFICI 49
6 ABBREVIAZIONI ED ACRONIMI 51

Sommario

Il progetto consiste nell'individuare e nell'analizzare le principali problematiche connesse alla protezione dei dati personali nell'ambito delle comunità energetiche pilota e delle correlate tecnologie abilitanti, a supporto dell'attività sperimentale condotta da ENEA e, più in generale, di coloro che intendano realizzare il nuovo modello, previsto anche a livello eurounitario, funzionale ad accelerare e agevolare la transizione energetica.

Il tema delle *energy communities* si interseca, infatti, con quello della *privacy,* perché il nuovo "schema" di produzione e di distribuzione dell'energia implica anche l'uso di dati personali per il suo funzionamento.

Si consideri, innanzitutto, che l'operatività delle nuove comunità sperimentali comporta l'acquisizione e la gestione di dati anagrafici, di contatto e di indirizzo di abitazione, conferiti dagli interessati aderenti, per l'esecuzione delle attività di installazione e di manutenzione dei sensori; nonché dei dati sui consumi elettrici, termici e sui valori ambientali, raccolti tramite i sensori installati presso le abitazioni degli interessati.

Del pari, il tema della privacy ricorre anche in caso di gestione dei dati forniti dagli utenti, tramite compilazione di una scheda-questionario, relativi alla loro abitazione, alle loro utenze e ai loro consumi, destinati a confluire in un'apposita piattaforma *web*.

La necessità di trattare legittimamente i dati personali emerge anche in caso di creazione di un'infrastruttura digitale per far emergere una serie di *feedback* per incrementare la "consapevolezza energetica" degli utenti, funzionante tramite *back-end* costituito da un *data-lake*.

Al contempo, eguale necessità sussiste in caso di realizzazione di un'apposita piattaforma, dedicata alla *local token economy*, in cui l'utente/aderente (che può essere o meno membro di una comunità energetica) può produrre e/o consumare servizi, di natura energetica/sociale, gestiti in un "*market place* digitale", che, tramite la tecnologia *blockchain*, consente l'incontro di domanda ed offerta, per la realizzazione di un modello mutualistico, cooperativo e sostenibile.

Del pari, l'attenzione alla disciplina sulla privacy è richiesta anche in caso di predisposizione di una piattaforma in grado di monitorare i *social media web* per estrarre alcune conoscenze (afferenti le comunità energetiche) senza alcuna supervisione umana.

L'obiettivo del progetto consiste, quindi, nel delineare, in prospettiva giuridica, il rapporto intercorrente tra *energy communities* e trattamento dei dati.

L'esigenza è, infatti, quella di conciliare l'innovazione legata all'uso delle nuove tecnologie – e i vantaggi apportati dalla creazione di nuove comunità in grado di contribuire all'efficientamento energetico – con la sicurezza dei dati personali.

Del resto, il flusso dei dati scaturente dal nuovo modello, giuridicamente riconosciuto, delle *energy communities* dovrebbe avvenire nel rispetto della disciplina a tutela dei dati personali, per come innovata dal Regolamento Generale sulla Protezione dei Dati, ossia il Regolamento UE 2016/679 (*General Data Protection Regulation* o *GDPR*).

Se, come evidenziato dal Rapporto "Comunità rinnovabili" di Legambiente, pubblicato nel 2020, "in tutto il mondo le comunità energetiche sono la frontiera della ricerca e delle applicazioni", perché espressione di un nuovo sistema energetico, democratico e sostenibile, allora sembra opportuno, a tutela degli utenti, individuare e tentare di neutralizzare anche i possibili rischi, sotto il profilo del trattamento dei dati personali, che potrebbero scaturire dall'adozione del modello.

La ricerca giuridica dell'Università degli Studi della Basilicata intende, pertanto, inquadrare e ricostruire, a partire dalla normativa vigente, le principali problematiche in tema di privacy in relazione alle comunità energetiche, anche sulla base delle questioni emerse nell'ambito delle sperimentazioni legate alla specifica ricerca, al fine di supportare la nascita e il funzionamento efficace del modello nelle sue diverse e possibili articolazioni.

1 Introduzione

Il tema delle comunità energetiche sembrerebbe, *prima facie*, del tutto avulso dalle questioni connesse alla tutela della privacy.

In realtà, i due argomenti sono strettamente correlati, al punto che la piena riuscita del modello delle *energy communities*, come si avrà modo di evidenziare, dipende dalla risoluzione di non pochi dubbi correlati al corretto uso dei dati personali che ne consentono il funzionamento.

Per spiegare i "punti di contatto" – e di possibile frizione – con la privacy, diritto che trova tutela sovranazionale nell'art. 8 della Carta dei diritti fondamentali dell'Unione e 16 del Trattato sul funzionamento dell'Unione europea (TFUE) [1], è necessario inquadrare, seppur nei limiti di quanto utile alla presente ricerca, il sistema delle comunità energetiche.

Occorre evidenziare, innanzitutto che, almeno in Europa, il modello (seppur embrionale e "rudimentale") della comunità energetica, inteso – in via di prima approssimazione – come "schema" di condivisione dell'energia da parte dei componenti di una collettività, ha una tradizione piuttosto risalente (si pensi, in Italia, alla Società Elettrica in Morbegno, fondata nel 1897).

Di recente, però, l'esigenza di procedere speditamente verso nuove forme di produzione e di consumo di energia, ispirate al principio di sostenibilità, in sostituzione delle fonti energetiche "tradizionali", limitate e inquinanti, ha indotto l'Unione europea a normare le comunità energetiche.

Il "pacchetto normativo" adottato dalle Istituzioni UE tra la fine del 2018 e la prima metà del 2019 (il c.d. "*Winter package*" o "*Clean energy package*") per individuare il quadro regolatorio per l'energia e il clima, ha introdotto, infatti, una prima disciplina eurounitaria per promuovere progetti energetici comunitari (riconducibili alla c.d. "*community energy*") nell'ambito dei quali le comunità energetiche, così come l'autoconsumo collettivo, svolgono un ruolo essenziale [2]. Si tratta, infatti, di modelli indispensabili per trasformare l'attuale sistema di produzione dell'energia elettrica centralizzato e alimentato da combustibili fossili, in un meccanismo decentrato, basato prevalentemente sulle energie "pulite" e, dunque, sostenibile, oltre che in grado di realizzare un nuovo paradigma di mercato energetico.

Il sistema delle *energy communities*, per come ideato a livello UE, costituisce un "baluardo" per il raggiungimento degli obiettivi di neutralità climatica e di accesso universale all'energia.

A tale riguardo, occorre evidenziare che la Direttiva 2018/2001/UE dell'11 dicembre 2018, sulla promozione dell'uso dell'energia da fonti rinnovabili (c.d. Direttiva RED II) introduce delle norme sugli autoconsumatori di energia da fonti rinnovabili (con la precisazione che, ai sensi dell'art. 2, par. 14, è "autoconsumatore di energia rinnovabile" il "cliente finale che, operando in propri siti situati entro confini definiti o, se consentito da uno Stato membro, in altri siti, produce energia elettrica rinnovabile per il proprio consumo e può immagazzinare o vendere energia elettrica rinnovabile autoprodotta purché, per un autoconsumatore di energia rinnovabile diverso dai nuclei familiari, tali attività non costituiscano l'attività commerciale o professionale principale"; con la precisazione che gli "autoconsumatori di energia rinnovabile che agiscono collettivamente" sono un "gruppo di almeno due autoconsumatori di energia rinnovabile che agiscono collettivamente (…) nello stesso edificio o condominio") e sulle comunità di energia rinnovabile (o "CER", ossia, ai sensi dell'art. 2, par. 16, il "soggetto giuridico: a) che, conformemente al diritto nazionale applicabile, si basa sulla partecipazione aperta e volontaria, è autonomo ed è effettivamente controllato da azionisti o membri che sono situati nelle vicinanze degli impianti di produzione di energia da fonti rinnovabili che appartengono e sono sviluppati dal soggetto giuridico in questione; b) i cui azionisti o membri sono persone fisiche, PMI o autorità locali, comprese le amministrazioni comunali; c) il cui obiettivo principale è fornire benefici ambientali, economici o sociali a livello di comunità ai suoi azionisti o membri o alle aree locali in cui opera, piuttosto che profitti finanziari". Di conseguenza, nell'ambito della comunità energetica l'autoconsumo collettivo trascende l'ambito di un unico edificio o condominio).

La qualifica di "soggetto giuridico" con una struttura "aperta" e a partecipazione "volontaria", avente come scopo principale non la realizzazione di profitti finanziari, ma il conseguimento di benefici ambientali, economici e sociali, costituisce elemento che accomuna le CER alle Comunità Energetica dei Cittadini (o

"CEC"), introdotte dalla Direttiva UE 2019/944 del 5 giugno 2019 (c.d. Direttiva IEM), sul mercato elettrico interno (secondo cui, ai sensi dell'art. 2, par. 10, la CEC è il "soggetto giuridico che: a) è fondato sulla partecipazione volontaria e aperta ed è effettivamente controllato da membri o soci che sono persone fisiche, autorità locali, comprese le amministrazioni comunali, o piccole imprese; b) ha lo scopo principale di offrire ai suoi membri o soci o al territorio in cui opera benefici ambientali, economici o sociali a livello di comunità, anziché generare profitti finanziari; e c) può partecipare alla generazione, anche da fonti rinnovabili, alla distribuzione, alla fornitura, al consumo, all'aggregazione, allo stoccaggio dell'energia, ai servizi di efficienza energetica, o a servizi di ricarica per veicoli elettrici o fornire altri servizi energetici ai suoi membri o soci").

Da un raffronto tra gli artt. 21-22 della Direttiva 2018/2001/UE e l'art. 16 della Direttiva 2019/944/UE emerge, però, che, a differenza della CEC, la CER è caratterizzata dal principio di autonomia tra i membri, dalla necessità di prossimità con gli impianti di generazione e dalla gestione di forme diverse di energia (elettricità, calore, gas), purché generate da una fonte rinnovabile (al contrario, la CEC può gestire solo l'elettricità, prodotta da fonte rinnovabile o fossile).

Ad ogni modo, si tratta di forme di "emancipazione" energetica, basate sulla delocalizzazione e sulla decentralizzazione della produzione e dello stoccaggio dell'energia.

La previsione eurounitaria di tali nuovi istituti assolve, dunque, la finalità di valorizzare la produzione e la distribuzione di energia in prossimità della domanda e delle utenze finali, tramite impianti di piccole-medie dimensioni gestiti direttamente dagli utilizzatori (famiglie, condomini, piccole e medie imprese, nuclei sociali composti da un numero esiguo di individui) [3].

In questo modo, il legame utente-energia muta al punto tale da realizzare un nuovo modello di gestione e produzione energetica, in grado non solo di produrre benefici ambientali, ma anche di generare un innovativo micro-sistema economico, basato sull'aggregazione.

In Italia, nelle more del recepimento di tale Direttiva 2018/2001/UE, che sarebbe dovuto avvenire entro giugno 2021, il legislatore ha previsto una disciplina sperimentale dei nuovi "schemi" funzionali alla transizione energetica. In particolare l'art. 42-*bis* ("Autoconsumo da fonti rinnovabili") della legge 28 febbraio 2020, n. 8, introdotto tramite emendamento in sede di conversione del d.l. 30 dicembre 2019, n. 162 (c.d. decreto Milleproroghe) ha provvisoriamente disciplinato l'autoconsumo collettivo da fonti rinnovabili e la nascita delle comunità energetiche rinnovabili.

L'attuazione della normativa è avvenuta con la delibera 318/2020/R/eel dell'Autorità di regolazione per energia reti e ambiente (ARERA) che, dopo aver fornito le definizioni di "autoconsumatore" e "comunità di comunità di energia rinnovabile", nonché di "produttore" e di "referente", individua i requisiti per l'accesso al servizio di valorizzazione e incentivazione dell'energia elettrica condivisa e la relativa procedura, incluso il ruolo-chiave del Gestore dei servizi energetici (GSE). Al contempo, la delibera appena citata pone le basi per l'erogazione (tramite una procedura unificata, come previsto dal decreto Milleproroghe) degli incentivi per il servizio di energia condivisa, definiti dal Ministero dello sviluppo economico (MISE), con decreto ministeriale del 16 settembre 2020 ed entrato in vigore il 17 novembre 2020.

Con la determina n. 6/2020, l'ARERA ha poi approvato le regole tecniche GSE sugli incentivi all'energia condivisa in comunità energetiche o autoconsumo collettivo, pubblicate il 22 dicembre 2020, che individuano i requisiti, le modalità di richiesta per l'accesso al servizio, lo schema di contratto standard, i criteri di calcolo e le tempistiche di erogazione dei contributi economici.

Da ultimo, seppur con ritardo, la disciplina eurounitaria sulle comunità energetiche è stata trasposta nel nostro ordinamento con il d.lgs. 8 novembre 2021, n. 199, recante "Attuazione della direttiva (UE) 2018/2001 del Parlamento europeo e del Consiglio, dell'11 dicembre 2018, sulla promozione dell'uso dell'energia da fonti rinnovabili".

Tra le novità più rilevanti rispetto alla disciplina contenuta nel Milleproroghe si segnala la possibilità di realizzare impianti di potenza più elevata, fino a 1 MW, anziché i 200 kW precedentemente previsti, e

l'afferenza di tutti i membri a una cabina primaria, che copre aree più ampie e, dunque, estende il perimetro dell'iniziativa, rispetto a quella secondaria.

In tal modo, la nuova normativa rafforza il modello della comunità energetica, potenzialmente in grado di coinvolgere un numero più elevato di individui e di realizzare impianti con investimenti e, dunque, con ricadute più rilevanti rispetto a quanto previsto nelle disposizioni provvisoriamente introdotte.

Per un quadro normativo completo sulle comunità energetiche e sul loro ruolo nel nostro sistema giuridico, si consideri, inoltre, che il c.d. Superbonus del 110% – rientrante tra le misure urgenti in materia di salute, di sostegno al lavoro e all'economia, nonché di politiche sociali connesse all'emergenza epidemiologica da COVID-19, previste dal d.l. 19 maggio 2020, n. 34 (c.d. decreto Rilancio), come convertito nella l. 17 luglio 2020, n. 77 – è esteso "all'installazione degli impianti fotovoltaici fino a 200 kW, da parte di comunità energetiche rinnovabili costituite in forma di enti non commerciali o da parte di condomìni, in presenza di requisiti specifici, anche se corrisponde solo alla quota di spesa corrispondente alla potenza massima di 20 kW".

In tale contesto, nell'ambito delle risorse della "Missione 2" («Rivoluzione verde e transizione ecologica»), il Piano Nazionale di Ripresa e Resilienza «Italia Domani» prevede un investimento di 2 miliardi e 200 milioni di euro per la promozione delle comunità energetiche e dell'autoconsumo collettivo, con focus sulle aree di "maggiore impatto socio-territoriale", al fine di sostenere le pubbliche amministrazioni, le famiglie e le microimprese che si aggregano, a livello di condominio o di quartiere, in Comuni con meno di 5.000 abitanti.

L'obiettivo è quello di installare circa 2.000 MW di nuova capacità di generazione elettrica configurata in modo distribuito, per ridurre le emissioni gas serra, promuovere l'economia micro-locale e favorire l'inclusione sociale[4].

I nuovi modelli, funzionali a una trasformazione energetica (e non solo) "a partire dal basso", basati sulla figura inedita del "*prosumer*", ossia sull'utente che non svolge solo il ruolo consumatore, ma partecipa attivamente alla produzione dell'energia "pulita", e sul connubio tra nuove tecnologie e consumo sostenibile dell'energia, pongono problemi, in parte inediti, anche a livello giuridico.

Tra le questioni più rilevanti per l'implementazione delle *energy communities* e delle soluzioni di autoconsumo collettivo vi è quella relativa alla corretta gestione, dal punto di vista giuridico, del flusso di dati che ne permette e connota l'operatività.

Del resto, le comunità energetiche sono anche comunità di dati [5], non di rado personali, ossia, almeno indirettamente, riconducibili a una persona fisica, ai sensi dell'art. 4 del GDPR (su cui si rinvia *infra*).

Il *data processing* è, infatti, indispensabile per il funzionamento dei nuovi modelli e soluzioni elaborati per la transizione energetica.

L'operatività delle comunità energetiche (o, in ogni caso, dell'autoconsumo collettivo) comporta, innanzitutto, una lettura ad alta frequenza della produzione e del consumo energetico, tramite la dotazione di *smart meters* (ossia dei c.d. contatori intelligenti).

Si consideri, inoltre, che i dispositivi intelligenti che comunicano con i sensori, per ridurre l'impiego di energia, si basano, a loro volta, sulla raccolta, sul monitoraggio e sulla gestione dei dati delle utenze, che vengono analizzati per fornire dei suggerimenti di ottimizzazione dei consumi.

In questo contesto devono essere considerati gli strumenti sviluppati dall'ENEA in grado di fornire delle analisi preliminari di tipo energetico, economico e finanziario in ambito residenziale, o l'implementazione di piattaforme *Internet of Things* (*IoT*) funzionali a raccogliere, ad aggregare e ad analizzare dati, con la possibilità di fornire un *feedback* all'utente per ridurre il consumo energetico.

Il tema dei rapporti tra comunità energetiche e tutela della privacy si complica ulteriormente se si considera che le prime possono essere la base di un modello di *sharing economy*. Le comunità – non più solo energetiche – divengono, infatti, anche il substrato di una vera e propria rete di scambi di beni e di servizi, basata sulla *local token economy* (LEC), ossia su *microgrid* virtuale "*peer to peer*" (funzionante con un'infrastruttura "tra pari").

Il modello LEC si basa sulla *blockchain* (letteralmente "catena di blocchi"), ossia – in via di prima approssimazione – una gamma di tecnologie basate su una rete informatica di pc, i c.d. nodi, in grado di validare, in modo sicuro, verificabile e tendenzialmente immutabile, un registro contenente dati e *smart contracts*, ossia *software* che, se installati sulla "catena di blocchi", consentono di concludere automaticamente dei contratti al verificarsi di determinate condizioni.

Blockchain e *smart contract* costituiscono, dunque, nuove soluzioni tecnologiche, riconosciute dal legislatore italiano, con la legge 11 febbraio 2019, n. 121, di conversione, con modificazioni, del decreto-legge 14 dicembre 2018, n. 135 (recante disposizioni urgenti in materia di sostegno e semplificazione per le imprese e per la pubblica amministrazione).

Al contempo, tramite apposita piattaforma, è possibile monitorare i *social media web* per estrarre informazioni sulle comunità energetiche, senza alcuna supervisione umana.

Le tecnologie abilitanti elaborate in via sperimentale da ENEA sono tenute, dunque, a un'ulteriore "sfida", ossia quella della piena *compliance* con la disciplina a tutela del trattamento dei dati personali.

2 Descrizione delle attività svolte e risultati

La ricerca giuridica ha lo scopo di individuare le principali questioni derivanti dalle applicazioni concrete del GDPR nella sperimentazione delle nuove comunità energetiche.

A tale fine, con scelta condivisa da ENEA, si è ritenuto opportuno tracciare un "*vademecum* della *privacy*", ossia uno strumento agile e di pronta consultazione, in grado di fornire un ausilio effettivo nel trattamento dei dati personali nel contesto, sperimentale e inedito, delle *energy communities*.

L'obiettivo è quello di delineare una "guida operativa" – che costituisce la parte esplicativa di una tabella (o *check list*) e di una *flowchart* – in grado di descrivere gli aspetti salienti della disciplina posta a tutela dei dati personali, con esempi a corredo dell'impianto teorico, rappresentati dai casi d'uso previsti nel modello di comunità energetica che ENEA intende sviluppare.

Per la complessità e per l'ampiezza della materia, senza pretesa di esaustività, il "*vademecum*", la correlata *check list* e la *flowchart* vorrebbero costituire un primo supporto pratico per consentire a tutti coloro che sono impegnati nello svolgimento di attività relative alle operazioni di trattamento dei dati personali nell'ambito delle comunità energetiche di orientarsi nella normativa in tema di privacy.

Tali strumenti potrebbero essere di ausilio anche pro futuro per agevolare e accelerare il dialogo tra i ricercatori/tecnici e il *Data protection officer* (DPO o Responsabile della Protezione Dati) di riferimento .

Di conseguenza, la "guida" può contribuire a incrementare la consapevolezza della tutela da garantire agli aventi diritto, degli obblighi da rispettare e degli adempimenti necessari per conformarsi alla disciplina prevista dal GDPR, nel contesto delle comunità energetiche.

Ad ogni modo, occorre evidenziare che il "*vademecum*" è un supporto sintetico, per cui, prima di procedere a un'attività che comporti il trattamento dei dati personali, già in fase di progettazione della sperimentazione, si suggerisce di consultare sempre il DPO e di approfondire ogni aspetto trattato nella presente ricerca, da aggiornare periodicamente, attraverso il sito web dell'Autorità Garante per la protezione dei dati personali [6].

A tale proposito, pare opportuno segnalare anche la "Guida all'applicazione del Regolamento europeo in materia di protezione dei dati personali", pubblicata sul sito del Garante della privacy [7], in cui sono individuate le questioni principali che i soggetti pubblici e privati devono tenere in considerazione nell'applicazione del GDPR.

In via preliminare, occorre evidenziare, invero, che né le citate Direttiva RED II e IEM, né il c.d. decreto Milleproroghe, né la disciplina nazionale di recepimento contengono delle disposizioni *ad hoc* sul tema del trattamento dati personali nell'ambito delle comunità energetiche.

Pare opportuno sottolineare, inoltre, che il Regolamento generale, nonostante sia un avanzato strumento di regolazione, funzionale a rafforzare la strategia eurounitaria per la creazione del mercato unico digitale, non affronta talune questioni emerse con la diffusione delle nuove tecnologie e dei sistemi di decisione algoritmica utilizzati in alcune ipotesi di trattamento dei dati personali.

Del resto, il Regolamento è un testo normativo destinato a rimodularsi in relazione all'evoluzione sociale e – soprattutto – tecnologica, tant'è che lo stesso art. 97 del GDPR ne prevede un riesame con cadenza quadriennale, così da consentire alla Commissione dell'Unione europea di proporre modifiche, tenuto conto, "in particolare, degli sviluppi delle tecnologie dell'informazione e dei progressi della società dell'informazione". Al riguardo, pare opportuno segnalare anche che il 4 aprile 2021 le Autorità europee per la protezione dei dati (il c.d. Gruppo Articolo 29) hanno espresso parere favorevole sulla proposta di Regolamento della Commissione europea concernente il "rispetto della vita privata e la protezione dei dati personali nelle comunicazioni elettroniche all´interno dell´Unione Europea" (il c.d. Regolamento *ePrivacy*).

Al contempo, nel sistema regolatorio in tema di privacy, il GDPR non può essere considerato come una "monade". Nel nostro ordinamento, infatti, assumono rilevanza anche gli strumenti c.d. di *soft law* (per esempio, i codici di condotta, le regole deontologiche e le linee guida), i meccanismi deputati all'applicazione uniforme della disciplina espressamente previsti nel Capo VII del GDPR, rubricato "Cooperazione e coerenza"

e la Direttiva 2002/58/CE (c.d. Direttiva *e-privacy*), per come revisionata dalla Direttiva 2009/136/CE, sul trattamento dei dati personali nell'ambito delle comunicazioni elettroniche.

Il GDPR non ha comportato, inoltre, l'abrogazione del Codice in materia di trattamento dei dati personali (ossia del d.lgs. 30 giugno 2003, n. 196), ma l'aggiornamento e l'adeguamento della normativa interna, avvenuti tramite le modifiche introdotte dal d.lgs. 10 agosto 2018, n. 101 [8].

Senza contare il ruolo del Comitato Europeo per la Protezione dei Dati (EDPB - *European Data Protection Board*), organo europeo indipendente, che contribuisce all'applicazione coerente delle norme sulla protezione dei dati in tutta l'Unione europea e promuove la cooperazione tra le autorità competenti per la protezione dei dati dell'UE, e dell'Autorità Garante della Privacy.

A livello internazionale, peraltro, occorre evidenziare che il 18 maggio 2018, a Elsinore, è stato adottato il protocollo alla Convenzione sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale. Il 5 marzo 2019 l'Italia ha sottoscritto tale protocollo e, con la legge 22 aprile 2021 n. 60, il Parlamento italiano ne ha autorizzato la ratifica ed esecuzione.

In via generale, viste le finalità delle sperimentazioni in atto, si consiglia di consultare preliminarmente le Regole deontologiche per trattamenti a fini statistici o di ricerca scientifica pubblicate ai sensi dell'art. 20, comma 4, del d.lgs. 10 agosto 2018, n. 101, adottate dal Garante del Privacy.

In questo contesto, piuttosto frammentario e disorganico, la ricerca intende contribuire alla realizzazione di un "percorso guidato" per la protezione dei dati personali nell'ambito delle comunità energetiche di nuova sperimentazione.

2.1 1° step: individuare il trattamento di dati personali

La prima operazione da compiere consiste nel comprendere se l'attività che si intende porre in essere comporta il trattamento di dati personali.

A tale fine, è necessario comprendere, rispettivamente, cosa si intenda per "trattamento" e per "dati personali" [9].

L'articolo 4 del GDPR definisce il trattamento dei dati personali come "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".

Il concetto di trattamento è, dunque, piuttosto ampio e include tutte le operazioni che implicano una conoscenza di dati personali.

L'articolo 2 del GDPR chiarisce che la disciplina ivi prevista si applica a due tipi di trattamenti di dati personali: quelli interamente o parzialmente automatizzati; quelli non automatizzati ("su carta") afferenti a dati personali contenuti in un archivio o destinati a figurarvi.

L'ambito di applicazione del GDPR si ricava anche "in negativo", come desumibile dal considerando 18, ai sensi del quale il regolamento europeo "non si applica al trattamento di dati personali effettuato da una persona fisica nell'ambito di attività a carattere esclusivamente personale o domestico e quindi senza una connessione con un'attività commerciale o professionale. Le attività a carattere personale o domestico potrebbero comprendere la corrispondenza e gli indirizzari, o l'uso dei *social network* e attività online intraprese nel quadro di tali attività".

Il medesimo considerando stabilisce, tuttavia, che il GDPR "si applica ai titolari del trattamento o ai responsabili del trattamento che forniscono i mezzi per trattare dati personali nell'ambito di tali attività a carattere personale o domestico".

Pare opportuno evidenziare, inoltre, che, se un'attività richiede più trattamenti di dati personali, ciascuno di essi dovrà ricevere specifica e puntuale considerazione.

Occorre considerare, inoltre, la perdurante vigenza della citata Direttiva 2002/58/CE, sulla tutela della vita privata nel settore delle comunicazioni elettroniche, anche definita "Direttiva *e-Privacy*", per come modificata dalla Direttiva 2009/136/CE.

Questa disciplina ha un campo di applicazione molto più ristretto rispetto a quello del GDPR, perché riguarda il trattamento dei dati personali connesso alla fornitura di servizi di comunicazione elettronica accessibili al pubblico su reti pubbliche di comunicazione nella Comunità, comprese le reti di comunicazione pubbliche che supportano i dispositivi di raccolta e di identificazione dei dati (ad es., in caso di servizi dei motori di ricerca che prevedono la memorizzazione di o l'accesso a marcatori o "*cookies*").

Ai sensi dell'art. 2, lett. c), della versione attuale della Direttiva quadro, il "servizio di comunicazione elettronica" include, infatti, "i servizi forniti di norma a pagamento consistenti esclusivamente o prevalentemente nella trasmissione di segnali su reti di comunicazioni elettroniche, compresi i servizi di telecomunicazioni e i servizi di trasmissione nelle reti utilizzate per la diffusione circolare radiotelevisiva, ma ad esclusione dei servizi che forniscono contenuti trasmessi utilizzando reti e servizi di comunicazione elettronica o che esercitano un controllo editoriale su tali contenuti; sono inoltre esclusi i servizi della società dell'informazione di cui all'articolo 1 della direttiva 98/34/CE100 non consistenti interamente o prevalentemente nella trasmissione di segnali su reti di comunicazione elettronica".

Fatte salve le fattispecie disciplinate in modo esclusivo ed esaustivo dalla Direttiva *e-Privacy*, in virtù del carattere speciale di quest'ultima rispetto alla normativa contenuta nel Regolamento – desumibile dall'art. 1, par. 2, della direttiva – ogniqualvolta il trattamento ricade nell'ambito di applicazione di entrambi, in quanto *lex specialis*, essa prevale sulle (più generali) disposizioni del GDPR. Le norme di quest'ultimo si applicano, invece, in tutte quelle fattispecie non specificamente previste dalla Direttiva, nonché quale cornice regolatoria generale entro cui collocarne i precetti.

Ai sensi dell'art. 4, par. 1, n. 1, per dato personale si intende "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".

Come specificato dal Gruppo di lavoro articolo 29, nell'ambito del parere n. 4/2007, può trattarsi di "informazioni "oggettive" come la presenza di una data sostanza nel sangue di una persona, ma anche informazioni "soggettive" come opinioni o valutazioni".

A titolo esemplificativo, i dati personali che potrebbero essere trattati nell'ambito di una comunità energetica sono i seguenti:

i) dati identificativi o anagrafici, ossia nome, cognome, indirizzo e-mail, numero di telefono, codice fiscale, ragione sociale, ecc.;

ii) dati di contatto e di navigazione/dati identificativi dell'utente, come, ad esempio, il nome dell'*Internet Service Provider* e l'indirizzo del Protocollo Internet (IP), la data e l'ora della richiesta, il codice numerico indicante la risposta fornita dal server, contenuto dei messaggi inviati, altri dati forniti durante le comunicazioni – anche telefoniche – intercorse;

iii) dati forniti volontariamente dall'utente – informazioni identificative – per l'accesso ai servizi offerti tramite sito web/piattaforma, da individuare in apposite informative presenti nelle sezioni di riferimento.

iv) dati contrattuali, ossia i dati necessari per la stipulazione e per l'esecuzione di contratti per lo scambio di beni e di servizi nell'ambito di un *marketplace* (concernenti, ad esempio, informazioni che riguardano il sottoscrittore, il beneficiario del servizio o il destinatario della consegna del bene, come il numero della carta di credito o l'indirizzo della sua casa).

v) dati di consumo, ossia i dati relativi alla fornitura e ai livelli di consumo registrati, raccolti ed elaborati (in particolare, dati di consumo elettrico in un intervallo di tempo espressi in kWh), con l'avvertenza che più brevi sono gli intervalli di misurazione, maggiori saranno i dettagli sul profilo di consumo (e, dunque, dell'utente).

Potrebbero poi venire in rilievo i dati storici di fatturazione o quelli del profilo temporale di prelievo.

Con specifico riferimento agli *smart meters*, come evidenziato dal Gruppo di lavoro articolo 29 nell'ambito del parere adottato il 4 aprile 2011, n. 12, possono essere considerati oggetto di trattamento:

• "codice identificativo univoco del contatore intelligente e/o numero di riferimento univoco dell'immobile (in mancanza di tali elementi identificativi, il contatore può comunque essere identificato mediante il suo grafico specifico del carico energetico);

• metadati relativi alla configurazione del contatore intelligente;

• descrizione del messaggio che viene trasmesso, per esempio se si tratta di una lettura del contatore o di una segnalazione di manomissione;

• indicazione di data e ora;

• contenuto del messaggio".

Ad ogni modo, in caso di attività che comporti il trattamento dei dati personali, o in presenza di un minimo dubbio al riguardo, occorre coinvolgere immediatamente il *Data protection officer*.

2.2 2° step: individuare i dati personali trattati e se rientrano in "particolari categorie"

Premessa la definizione ampia di dati personali (evidenziata nel paragrafo precedente, al quale si rinvia), occorre sottolineare la distinzione tra: dati comuni (es. il nominativo, la data di nascita, il numero di cellulare, l'indirizzo e-mail, ecc.) e dati sensibili, che l'art. 9 del GDPR definisce come "particolari categorie di dati". Si tratta dei dati personali che rivelano "l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona".

Il distinguo tra dati personali comuni e "sensibili" [10] rileva in punto di disciplina.

La normativa stabilisce, infatti, un divieto generale di trattare queste categorie di dati, salvo alcune eccezioni, perché il loro contenuto è tale da creare un rischio significativo per i diritti e le libertà delle persone cui appartengono.

Ai sensi dell'art. 9, par. 2, del GDPR, dunque, i dati particolari (o "sensibili") possono essere trattati solo se:

"a) l'interessato ha prestato il proprio consenso esplicito al trattamento di tali dati personali per una o più finalità specifiche, salvo nei casi in cui il diritto dell'Unione o degli Stati membri dispone che l'interessato non possa revocare il divieto di cui al paragrafo 1;

b) il trattamento è necessario per assolvere gli obblighi ed esercitare i diritti specifici del titolare del trattamento o dell'interessato in materia di diritto del lavoro e della sicurezza sociale e protezione sociale, nella misura in cui sia autorizzato dal diritto dell'Unione o degli Stati membri o da un contratto collettivo ai sensi del diritto degli Stati membri, in presenza di garanzie appropriate per i diritti fondamentali e gli interessi dell'interessato;

c) il trattamento è necessario per tutelare un interesse vitale dell'interessato o di un'altra persona fisica qualora l'interessato si trovi nell'incapacità fisica o giuridica di prestare il proprio consenso;

d) il trattamento è effettuato, nell'ambito delle sue legittime attività e con adeguate garanzie, da una fondazione, associazione o altro organismo senza scopo di lucro che persegua finalità politiche, filosofiche, religiose o sindacali, a condizione che il trattamento riguardi unicamente i membri, gli ex membri o le persone

che hanno regolari contatti con la fondazione, l'associazione o l'organismo a motivo delle sue finalità e che i dati personali non siano comunicati all'esterno senza il consenso dell'interessato;

e) il trattamento riguarda dati personali resi manifestamente pubblici dall'interessato;

f) il trattamento è necessario per accertare, esercitare o difendere un diritto in sede giudiziaria o ogniqualvolta le autorità giurisdizionali esercitino le loro funzioni giurisdizionali;

g) il trattamento è necessario per motivi di interesse pubblico rilevante sulla base del diritto dell'Unione o degli Stati membri, che deve essere proporzionato alla finalità perseguita, rispettare l'essenza del diritto alla protezione dei dati e prevedere misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato;

h) il trattamento è necessario per finalità di medicina preventiva o di medicina del lavoro, valutazione della capacità lavorativa del dipendente, diagnosi, assistenza o terapia sanitaria o sociale ovvero gestione dei sistemi e servizi sanitari o sociali sulla base del diritto dell'Unione o degli Stati membri o conformemente al contratto con un professionista della sanità, fatte salve le condizioni e le garanzie di cui al paragrafo 3;

i) il trattamento è necessario per motivi di interesse pubblico nel settore della sanità pubblica, quali la protezione da gravi minacce per la salute a carattere transfrontaliero o la garanzia di parametri elevati di qualità e sicurezza dell'assistenza sanitaria e dei medicinali e dei dispositivi medici, sulla base del diritto dell'Unione o degli Stati membri che prevede misure appropriate e specifiche per tutelare i diritti e le libertà dell'interessato, in particolare il segreto professionale;

j) il trattamento è necessario a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici in conformità dell'articolo 89, paragrafo 1, sulla base del diritto dell'Unione o nazionale, che è proporzionato alla finalità perseguita, rispetta l'essenza del diritto alla protezione dei dati e prevede misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato".

I dati personali di cui all'articolo 9 del GDPR possono essere trattati, inoltre, per la finalità di cui al punto h), se il trattamento avviene ad opera o sotto la responsabilità di un professionista soggetto al segreto professionale conformemente al diritto dell'Unione o degli Stati membri o alle norme stabilite dagli organismi nazionali competenti o da altra persona anch'essa soggetta all'obbligo di segretezza conformemente al diritto dell'Unione o degli Stati membri o alle norme stabilite dagli organismi nazionali competenti.

Ai nostri fini, occorre evidenziare che tra le ipotesi di liceità del trattamento delle "particolari categorie di dati" vi è quella legata alla ricerca scientifica (seppur alle condizioni specificate dal citato art. 9, par. 2, lett. j), del GDPR).

In occasione dell'adeguamento del Codice Privacy al GDPR, si è stabilito che l'autorità di controllo può imporre ulteriori misure di garanzia nel caso di trattamento dei dati sulla salute, i dati genetici o biometrici, tramite atti soggetti a revisione biennale (al riguardo, si rinvia al provvedimento del Garante della Privacy 5 giugno 2019, Prescrizioni relative al trattamento di categorie particolari di dati, ai sensi dell'articolo 21, comma 1 del decreto legislativo 10 agosto 2018, n. 101. (Provvedimento n. 146)).

Occorre poi menzionare la categoria dei dati giudiziari, che l'art. 10 del GDPR identifica in quelli relativi "alle condanne penali e ai reati o a connesse misure di sicurezza".

In tal caso, il trattamento è lecito solo se, sulla base dell'art. 6, par. 1, del GDPR (ossia quando l'interessato ha reso il consenso, per l'esecuzione di un contratto o di misure precontrattuali su richiesta dell'interessato, in base a obbligo di legge, per la salvaguardia di interessi vitali dell'interessato, per lo svolgimento di un compito di interesse pubblico, per il perseguimento di un legittimo interesse del titolare) è autorizzato dal diritto dell'Unione o dallo Stato membro, con garanzie appropriate per i diritti e le libertà degli interessati o, in alternativa, vi è il controllo dell'Autorità pubblica.

Pare opportuno evidenziare, inoltre, l'ultima parte del Considerando 26 del GDPR, secondo cui "i principi di protezione dei dati non dovrebbero […] applicarsi a informazioni anonime, vale a dire informazioni che non si riferiscono a una persona fisica identificata o identificabile o a dati personali resi sufficientemente anonimi da impedire o da non consentire più l'identificazione dell'interessato".

L'anonimizzazione, che ricorre esclusivamente quando il titolare non è in grado, in alcun modo, di re-identificare l'interessato, è una tecnica che consente di sottrarre l'informazione acquisita al GDPR.

L'anonimizzazione è, dunque, diversa dalla pseudonimizzazione: quest'ultima consiste, infatti, in un processo reversibile, che consente di re-identificare l'interessato, e non sottrae i dati acquisiti dalle tutele previste dal GDPR.

L'articolo 4, par. 5, del GDPR chiarisce, infatti, che per pseudonimizzazione si intende "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 considerando 26 del Regolamento sopracitato specifica, poi, che "I dati personali sottoposti a pseudonimizzazione, i quali potrebbero essere attribuiti a una persona fisica mediante l'utilizzo di ulteriori informazioni, dovrebbero essere considerati informazioni su una persona fisica identificabile […]"

Resta fermo che, come evidenziato dal considerando 28 del GDPR, "l'applicazione della pseudonimizzazione ai dati personali può ridurre i rischi per gli interessati e aiutare i titolari del trattamento e i responsabili del trattamento a rispettare i loro obblighi di protezione dei dati. L'introduzione esplicita della «pseudonimizzazione» nel presente regolamento non è quindi intesa a precludere altre misure di protezione dei dati."

La pseudonimizzazione è, infatti, una misura di sicurezza (articolo 32 del GDPR) e uno strumento a protezione dei dati (articolo 25 del GDPR).

Il considerando 29 del medesimo Regolamento afferma, inoltre, che "Al fine di creare incentivi per l'applicazione della pseudonimizzazione nel trattamento dei dati personali, dovrebbero essere possibili misure di pseudonimizzazione con possibilità di analisi generale all'interno dello stesso titolare del trattamento, qualora il titolare del trattamento abbia adottato le misure tecniche e organizzative necessarie ad assicurare, per il trattamento interessato, l'attuazione del presente regolamento, e che le informazioni aggiuntive per l'attribuzione dei dati personali a un interessato specifico siano conservate separatamente".

Per una disamina delle migliori tecniche di pseudonimizzazione e di anonimizzazione si rinvia al documento dell'Agenzia dell'Unione europea per la cibersicurezza (ENISA) concernente, per l'appunto, le "Tecniche di pseudonomizzazione e migliori pratiche" [11].

2.3 3° step: individuare il titolare (o i titolari) del trattamento, il responsabile e gli altri soggetti coinvolti

Secondo l'art. 4, par. 7 del GDPR il titolare del trattamento (o data controller) è "la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri".

Si tratta, dunque, di chi decide «perché» e «come» devono essere trattati i dati personali [12].

Il *data controller* riveste un ruolo cruciale nell'ambito del trattamento dati, al punto che il citato Regolamento pone al centro della disciplina in tema di privacy proprio il titolare e le sue responsabilità.

Il GDPR è incentrato, infatti, sul principio di *accountability*, che coinvolge, innanzitutto, il *data controller*, in termini di affidabilità, di *compliance*, di responsabilità, di approccio proattivo circa il continuo monitoraggio e l'aggiornamento delle misure adottate, nonché di massima attenzione sulla scelta di soggetti idonei, ai quali affidare il trattamento dei dati.

Ai sensi dell'art. 24 il titolare è tenuto a mettere in atto "misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al presente regolamento. Dette misure sono riesaminate e aggiornate qualora necessario".

Di conseguenza, da un lato, il modello delineato dal GDPR è basato sul rischio, gravante sul titolare che, per evitarne la verificazione, è indotto a valutare *ex ante* le caratteristiche del trattamento, il grado di probabilità e di gravità delle potenziali conseguenze pregiudizievoli per l'interessato. L'approccio su cui si basa il GDPR dovrebbe indurre il titolare a progettare e a predisporre, innanzitutto, delle misure e delle cautele che, fin dall'inizio, consentano di azzerare, o almeno di limitare, il verificarsi di rischi per i dati personali dei soggetti coinvolti dal singolo e specifico trattamento (*privacy by design* e *by default*); dall'altro lato, il titolare non deve solo adottare misure adeguate rispetto alle norme in tema di privacy, ma deve essere anche in grado di documentarle (principio di trasparenza) e di garantirne l'efficacia, così da comprovare il rispetto dei principi sul trattamento dati.

Come evidenziato, infatti, il Regolamento si caratterizza per il principio della "responsabilizzazione" o "*accountability*", che impone ai titolari del trattamento di adottare comportamenti proattivi rispetto alla tutela dei dati personali e di dimostrare, in qualsiasi momento, l'efficacia delle misure organizzative e tecniche concretamente utilizzate.

In ragione anche delle modalità di gestione automatizzata dei dati personali, sempre più invasive e pervasive, il GDPR sancisce l'obbligo per i titolari di progettare i sistemi preposti al trattamento di dati che siano "*compliant*" con le prescrizioni del Regolamento (*privacy by design*) e di impostare, di *default*, il più elevato livello di protezione dei dati personali, ad esempio chiedendo all'interessato di validare il consenso (*privacy by default*) [13].

Sotto l'egida dei principi di integrità e di riservatezza, il titolare ha l'obbligo giuridico di garantire un livello di sicurezza adeguato ai dati personali oggetto del trattamento e, dunque, adottare misure di sicurezza, tecniche ed organizzative, idonee a proteggere i dati da trattamenti non autorizzati o illeciti e ad evitare il rischio della loro perdita, distruzione o danno accidentale. Il riferimento alla sicurezza include sia l'ambito giuridico amministrativo sia quello informatico, perché, oltre alla gestione delle informazioni e alla loro difesa da possibili intrusioni o alterazioni, è necessario implementare i sistemi di autorizzazione e di accesso al trattamento dei dati.

Al contempo, trovano conferma i principi generali sul trattamento dei dati personali già delineati dal previgente quadro normativo, ossia quelli di:

• liceità (ossia deve fondarsi su una base giuridica legittima), correttezza (inteso in termini di lealtà e buona fede, da osservare in tutte le fasi del trattamento, comprese quelle preparatorie o conclusive) e trasparenza (verso l'interessato, affinché, ad esempio, possa legittimamente fondare e manifestare il proprio consenso);

• integrità e riservatezza: i dati personali devono essere trattati in maniera da garantirne un'adeguata sicurezza/protezione;

• minimizzazione: i dati personali raccolti devono essere adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati;

• esattezza: i dati personali raccolti devono essere esatti e, se necessario, aggiornati, anche tramite la previsione di misure ragionevoli per cancellare o per rettificare tempestivamente le inesattezze riscontrate;

• limitazione delle finalità: i dati personali devono essere raccolti per finalità determinate, esplicite e legittime, per poi essere trattati in modo compatibile con esse o con il legittimo interesse del titolare. Per ogni diversa finalità deve essere richiesto uno specifico consenso all'interessato;

• limitazione della conservazione: i dati personali devono essere conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati (fermo restando che è ammessa la conservazione per periodi più lunghi, purché il trattamento sia esclusivamente a fini statistici, di archiviazione nel pubblico interesse, di ricerca scientifica o storica).

A tale fine, l'adesione ai codici di condotta, di cui all'art. 40 GDPR o a un meccanismo di certificazione, di cui all'art. 42 GDPR, può essere utilizzata come elemento per dimostrare l'osservanza dei principi e il rispetto degli obblighi gravanti sul titolare.

L'individuazione del titolare del trattamento è, dunque, di estrema importanza, ma non è sempre agevole. Ad esempio, in caso di *blockchain*, in astratto, il ruolo di *data controller* potrebbe spettare al programmatore o all'iniziatore dell'applicazione, a ogni partecipante che esegue una transazione, al "*miner*" (ossia ai c.d. "minatori" del meccanismo di validazione delle operazioni) oppure all'operatore del nodo [14]. Occorre valutare, dunque, di volta in volta, a seconda delle specificità del caso d'uso e delle caratteristiche della "catena di blocchi", chi possa rivestire, in concreto, il ruolo di titolare del trattamento dei dati personali [15].

Può accadere, inoltre, che lo stesso trattamento sia in contitolarità, ossia abbia più titolari.

Ai sensi dell'art. 26 del GDPR, questa ipotesi ricorre quando "due o più titolari del trattamento determinano congiuntamente le finalità e i mezzi del trattamento", ossia nel caso in cui la definizione del «perché» e del «come» devono essere trattati i dati personali avvenga in modo congiunto.

I contitolari sono tenuti a determinare, in modo trasparente, tramite un accordo interno, le rispettive responsabilità riguardo all'osservanza degli obblighi derivanti dal Regolamento, con particolare riferimento all'esercizio dei diritti dell'interessato.

In tal senso, devono essere definite le rispettive funzioni di comunicazione delle informazioni di cui agli articoli 13 e 14, salvo che – e nella misura in cui – le rispettive responsabilità siano determinate dal diritto dell'Unione o dello Stato membro cui i titolari sono soggetti. Tale accordo, il cui contenuto essenziale è messo a disposizione dell'interessato, deve riflettere adeguatamente i rispettivi ruoli e i rapporti con gli interessati. In ogni caso, l'interessato può esercitare i propri diritti nei confronti di ciascun titolare del trattamento.

Il titolare può, inoltre, essere coadiuvato dalla figura del Responsabile del trattamento definita ai sensi dell'art. 4, n. 8), GDPR come "la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento". La locuzione "per conto del titolare" lascia intendere che la nomina di un responsabile dipenda soltanto dalla decisione del titolare del trattamento e che si tratti, dunque, di una figura meramente eventuale.

Ad ogni modo, una volta nominato, il responsabile è un *alter ego* tecnicamente qualificato del titolare, anche in ragione dell'intensificazione degli adempimenti a suo carico, nonché dei livelli di responsabilità, funzionali a elevare il livello di protezione dei dati personale e a garantire una *compliance* adeguata ed efficace alla normativa sulla privacy.

A tale fine, il responsabile deve fornire al titolare tutte le informazioni necessarie al raggiungimento degli obiettivi di trattamento e assisterlo nelle attività di revisione e di ispezione, segnalandogli anche il rischio di violazioni delle norme del Regolamento.

Il ruolo di responsabile può essere affidato a soggetti giuridici che, ai sensi dell'art. 28 GDPR, presentino "garanzie sufficienti per mettere in atto misure tecniche ed organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del GDPR e garantisca la tutela dei diritti dell'interessato". Tali misure dovrebbero tenere conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché del rischio per i diritti e le libertà degli interessati, in conformità del Considerando n. 74 del Regolamento. L'art. 28 stabilisce, inoltre, che i trattamenti effettuati ad opera del responsabile "sono disciplinati da un contratto o da altro atto giuridico a norma del diritto dell'Unione o degli Stati membri".

Con riferimento alle definizioni appena delineate, si segnala che il 7 Settembre 2020 il Comitato europeo per la protezione dei dati personali ("CEPD"), ossia l'organismo dell'UE previsto dall'art. 68 del GDPR, costituito dal vertice dell'autorità di controllo per ciascuno Stato membro e dallo *European Data Protection Supervisor*, ha posto in consultazione pubblica (terminata il 19 Ottobre 2020) le Linee Guida 7/2020 sui concetti di titolare e responsabile nel GDPR [16].

Pare opportuno evidenziare, inoltre, che i titolari e i responsabili di trattamento che non abbiano meno di 250 dipendenti (come l'ENEA) devono tenere un registro delle operazioni di trattamento, in forma scritta (anche elettronica), da esibire – all'occorrenza – al Garante della protezione dei dati personali.

La funzione del registro non è solo quella di garantire la supervisione da parte dell'Autorità di controllo, ma anche per avere un quadro aggiornato dei trattamenti in essere, funzionale alla valutazione e analisi del rischio.

I contenuti minimi del registro del titolare sono indicati all'art. 30, par. 1, GDPR e consistono nelle informazioni seguenti:

"a) il nome e i dati di contatto del titolare del trattamento e, ove applicabile, del contitolare del trattamento, del rappresentante del titolare del trattamento e del responsabile della protezione dei dati;

b) le finalità del trattamento;

c) una descrizione delle categorie di interessati e delle categorie di dati personali;

d) le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, compresi i destinatari di paesi terzi od organizzazioni internazionali;

e) ove applicabile, i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale, compresa l'identificazione del paese terzo o dell'organizzazione internazionale e, per i trasferimenti di cui al secondo comma dell'articolo 49, la documentazione delle garanzie adeguate;

f) ove possibile, i termini ultimi previsti per la cancellazione delle diverse categorie di dati;

g) ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative di cui all'articolo 32, paragrafo 1".

Del pari, l'art. 30, par. 2, individua i contenuti minimi del registro del responsabile:

"a) il nome e i dati di contatto del responsabile o dei responsabili del trattamento, di ogni titolare del trattamento per conto del quale agisce il responsabile del trattamento, del rappresentante del titolare del trattamento o del responsabile del trattamento e, ove applicabile, del responsabile della protezione dei dati;

b) le categorie dei trattamenti effettuati per conto di ogni titolare del trattamento;

c) ove applicabile, i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale, compresa l'identificazione del paese terzo o dell'organizzazione internazionale e, per i trasferimenti di cui al secondo comma dell'articolo 49, la documentazione delle garanzie adeguate;

d) ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative di cui all'articolo 32, paragrafo 1".

Pare opportuno precisare che il distinguo tra il responsabile e il titolare del trattamento dei dati, netto in teoria, può rivelarsi arduo in concreto. Si consideri, ad esempio, che, in caso di *blockchain*, per parte della dottrina [17], gli utilizzatori della stessa potrebbero essere considerati come responsabili dei dati, a partire dal momento in cui decidono quale informazione è inclusa nella transazione e potrebbero essere considerati anche titolari, da quando i loro computer eseguono/gestiscono la catena di blocchi.

Per completezza, occorre poi individuare gli incaricati che trattano i dati personali, ossia coloro che effettuano materialmente le operazioni di trattamento (art. 2-quaterdecies del Codice della Privacy), nei limiti della mera esecuzione di compiti, e i destinatari ai quali possono essere comunicati i dati.

A tale riguardo, occorre evidenziare che il GDPR non prevede, invece, in modo espresso, la figura dell'incaricato, ma consente comunque di persone autorizzate al trattamento dei dati, sotto l'autorità diretta del titolare o del responsabile (art. 4, n. 10).

L'autorizzato è tenuto, dunque, a rispettare le istruzioni operative ricevute (art. 29 GDPR) e deve essere privo di autonomia (altrimenti è da considerare "responsabile") [18].

2.4 4° step: individuare gli interessati e garantire il rispetto dei loro diritti

Come emerge da quanto fin qui evidenziato, l'interessato (o *data subject*) è il destinatario della tutela predisposta dal Regolamento europeo per le operazioni di trattamento dei dati personali.

L'interessato è persona fisica identificata o identificabile al quale appartiene il dato personale (art 4, par. 1 GDPR), ossia colui "che può essere identificato, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione (…)".

Come specificato dal Considerando 14: "È opportuno che la protezione prevista dal presente regolamento si applichi alle persone fisiche, a prescindere dalla nazionalità o dal luogo di residenza, in relazione al trattamento dei loro dati personali. Il presente regolamento non disciplina il trattamento dei dati personali relativi a persone giuridiche, in particolare imprese dotate di personalità giuridica, compresi il nome e la forma della persona giuridica e i suoi dati di contatto".

Di conseguenza, nel nostro ordinamento, l'interessato alla tutela dei dati personali è tendenzialmente solo una persona fisica [19].

A tale riguardo, occorrono, però, delle precisazioni.

Ad esempio, secondo quanto evidenziato dal Gruppo di Lavoro Art. 29, nel citato parere 4/2007, con riferimento ai dati di contatto, rientra nell'ambito di tutela del GDPR l'e-mail aziendale del dipendente, nel caso in cui l'indirizzo di posta elettronica sia composto dal nome e dal cognome della persona fisica (es. nome.cognome@società.it).

"Il WP29 invita ad utilizzare i criteri di "contenuto", "scopo" e "risultato" per stabilire se le informazioni personali si riferiscono alla persona giuridica o meno. Nel caso del modulo, infatti, è ovvio che lo "scopo" del campo "nome" è quello di raccogliere i dati del dipendente, e così allo stesso modo per gli altri campi. Appare quindi inverosimile non sottoporre alla tutela del GDPR questi dati.

In molti casi i trattamenti automatizzati di dati personali non distinguono tra dati relativi a persone fisiche e quelli relativi a persone giuridiche. In tal modo finiscono per aggiungere ai profili delle persone fisiche dati che sono, invece, afferenti alla persona giuridica. In questi casi conviene trattare sempre l'insieme dei dati come fossero dati personali relativi a persone fisiche" [20].

Sul sito della Commissione europea, si legge, inoltre che, ferma la tendenziale inapplicabilità delle norme sulla protezione dei dati personali alle persone giuridiche, "le informazioni relative a società unipersonali possono costituire dati personali laddove consentono l'identificazione di una persona fisica" [21] (articoli 1, 2 e 3 Considerando (13), (14), (15), (18), (19) e (21) del GDPR; sentenza della Corte di giustizia del 9 marzo 2017, Manni, C-398/15).

Le indicazioni fornite a livello sovranazionale suggeriscono, dunque, l'opportunità di vagliare, di volta in volta e in modo cauto, l'ambito di applicazione soggettivo del trattamento che si intende porre in essere e, in caso di dubbio, ad assumere scelte prudenti, finalizzate a incrementare, anziché potenzialmente sottrarre, margini di tutela.

Occorre poi ricordare che la citata Direttiva 2002/58/CE (c.d. Direttiva *e-privacy*), sulle comunicazioni elettroniche, trova applicazione anche alle persone giuridiche, enti ed associazioni del capo 1 del titolo X del Codice civile, in quanto "contraenti".

Il GDPR riconosce all'interessato una serie di diritti, ossia: il diritto all'informazione; il diritto di accesso ai dati, il diritto all'oblio, il diritto di rettifica dei dati, il diritto di limitazione e di opposizione al trattamento e il diritto alla portabilità dei dati [22], il diritto a non subire profilazioni inconsapevoli, su cui ci si soffermerà *infra*.

Pare opportuno ricordare, che, per tutti i diritti, il termine per la risposta all´interessato è di un mese, estendibile fino a 3 mesi, in casi di particolare complessità.

Sono ammesse deroghe ai diritti riconosciuti dal GDPR, ma solo se fondate su norme nazionali, ai sensi dell´articolo 23 GDPR e di altri articoli relativi ad ambiti specifici (si vedano, in particolare, art. 17, paragrafo 3, per quanto riguarda il diritto alla cancellazione/"oblio", art. 83 - trattamenti di natura giornalistica e art. 89 - trattamenti per finalità di ricerca scientifica o storica o di statistica).

***i*) diritto all'informazione**

Nell'ambito dei diritti dell'interessato, assume particolare rilievo quello a un'adeguata informativa, ai sensi degli artt. 12, 13, 14 e 15, contenuti nella I sezione del Capo III, del GDPR, rubricata "Trasparenza e modalità".

La norma di apertura, ossia l'art. 12 del GDPR, correla il principio di trasparenza a ulteriori corollari, fra cui il c.d. principio di conoscibilità, desumibile dall'obbligo del titolare di notificare e fornire all'interessato tutte le informazioni relative al trattamento (artt. 13-14 GDPR). Nel novero di queste ultime rilevano, in particolare, le indicazioni sull'esistenza di un processo decisionale automatizzato, compresa la profilazione, nonché quelle sulla logica utilizzata e sulle conseguenze del trattamento. L'art. 13 del GDPR prevede, inoltre, numerosi elementi conoscitivi che il titolare o il responsabile sono tenuti obbligatoriamente a fornire all'interessato e stabilisce, in maniera concisa, trasparente, intelligibile e facilmente accessibile, con peculiare attenzione al caso in cui i destinatari siano dei minori. Occorre evidenziare, inoltre, che il trattamento è trasparente, chiaro e corretto, solo se l'informativa resa all'interessato sia esaustiva sulle caratteristiche di quest'ultimo e sulle relative finalità. L'informativa, infatti, deve rendere edotto il *data subject* sulle modalità di trattamento e sulle misure di sicurezza adottate nel rispetto dei principi di riservatezza, integrità e disponibilità dei dati. Al contempo, dall'informativa deve evincersi se il conferimento dei dati è obbligatorio o facoltativo e quali siano le conseguenze di un eventuale rifiuto a rendere disponibili i propri dati personali. Dall'informativa devono essere desumibili, inoltre, l'identità dei soggetti a cui i dati saranno comunicati o se saranno diffusi; l'indicazione dei diritti *ex* art. 7 del GDPR, in materia di consenso; l'individuazione del titolare e, se designato, del responsabile del trattamento; il periodo previsto per la conservazione dei dati o, quantomeno, i criteri utilizzati per stabilirne la durata. L'art. 14 specifica, altresì, che se i dati personali non sono raccolti direttamente presso l'interessato, nel documento devono essere indicati: l'identità e i dati di contatto del titolare del trattamento e, ove applicabile, del suo rappresentante; la base giuridica, ossia l'origine del trattamento, specificando, inoltre, la sussistenza del legittimo interesse; il possibile trasferimento dei dati personali in Paesi terzi e attraverso quali strumenti; il periodo di conservazione dei dati; il diritto dell'interessato di presentare un reclamo o un ricorso giurisdizionale all'Autorità di controllo; il diritto di accesso, di rettifica, di cancellazione e di portabilità dei dati.

Quando la base giuridica del trattamento consiste nel consenso, il titolare deve essere in grado di dimostrare che l'interessato lo ha prestato liberamente e con riguardo a un trattamento specifico (art. 71 GDPR) [23].

Non occorre che il consenso sia "documentato per iscritto", anche se questa modalità è quella che consente al *data controller* di adempiere più agevolmente ai suoi oneri probatori. Ad ogni modo, la forma di consenso "esplicita" è richiesta per i dati sensibili (art. 9 GDPR) e per le decisioni basate su trattamenti automatizzati (inclusa, dunque, la profilazione, *ex* art. 22 GDPR). Il consenso al trattamento deve essere richiesto prima che inizi il trattamento e, dunque, prima dell'acquisizione dei dati personali.

In ogni caso, il consenso deve essere libero, specifico, informato, inequivocabile e mai tacito o presunto.

L'interessato deve essere posto nella condizione di effettuare una scelta autenticamente libera e, dunque, di poter rifiutare o revocare il consenso senza subire pregiudizio.

Nel caso in cui il consenso sia espresso nell'ambito della sottoscrizione di un contratto, la richiesta deve essere chiaramente distinguibile rispetto al resto dell'atto, in modo comprensibile e facilmente accessibile, con linguaggio semplice e chiaro.

Ai fini della ricerca, pare opportuno evidenziare che la Corte di Cassazione, sez. I, 25/5/2021 n. 14381 [24], ha affermato che "in tema di trattamento di dati personali, il consenso è validamente prestato solo se espresso liberamente e specificamente in riferimento a un trattamento chiaramente individuato; ne segue che nel caso di una piattaforma *web* (con annesso archivio informatico) […] incentrata su un sistema di calcolo con alla base un algoritmo […], il requisito di consapevolezza non può considerarsi soddisfatto ove lo schema esecutivo dell'algoritmo e gli elementi di cui si compone restino ignoti o non conoscibili da parte degli interessati" (nella specie, utilizzato per determinare il *rating* reputazionale).

La sentenza sembra di particolare interesse, perché – trattandosi di un precedente autorevole – la giurisprudenza successiva potrebbe confermare la necessità della messa a disposizione dello schema dell'algoritmo e degli elementi che lo compongono per la validità del consenso reso dall'interessato al trattamento automatizzato. La questione risulta di particolare attualità anche perché gli algoritmi sono protetti quali segreti commerciali [25], in base alla Direttiva 2016/943/UE (c.d. Direttiva *trade secrets*) dell'Unione europea, attuata nel nostro ordinamento dal d.lgs. 11 maggio 2018, n. 63.

Ad ogni modo, pare opportuno ricordare che il consenso dell'interessato non è l'unica base giuridica legittimante il trattamento.

Ai sensi dell'art. 6 GDPR, infatti, la liceità del trattamento sussiste anche quando quest'ultimo è necessario: b) all'esecuzione di un contratto di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso; c) per l'adempimento di un obbligo legale al quale è soggetto il titolare;

d) per la salvaguardia degli interessi vitali dell'interessato o di un'altra persona fisica;

e) per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento;

f) per il perseguimento del legittimo interesse del titolare del trattamento o di terzi (adeguatamente bilanciato con gli altri interessi in gioco).

***ii*) diritto di accesso**

Il diritto accesso da parte dell'interessato, *ex* art. 15 del GDPR, risponde al principio di trasparenza e comporta il diritto di ricevere una copia dei dati personali oggetto di trattamento. Il diritto di accesso ha, dunque, natura conoscitiva e "statica", perché basato sulla richiesta dell'interessato a ottenere dal titolare informazioni sul trattamento e sui dati trattati, con contestuale visibilità dei degli stessi.

Al riguardo, pare opportuno evidenziare quanto previsto dal Considerando 63 del GDPR, secondo cui "Un interessato dovrebbe avere il diritto di accedere ai dati personali raccolti che la riguardano e di esercitare tale diritto facilmente e a intervalli ragionevoli, per essere consapevole del trattamento e verificarne la liceità. Ciò include il diritto di accedere ai dati relativi alla salute, ad esempio le cartelle mediche contenenti informazioni quali diagnosi, risultati di esami, pareri di medici curanti o eventuali terapie o interventi praticati. Ogni interessato dovrebbe pertanto avere il diritto di conoscere e ottenere comunicazioni in particolare in relazione alla finalità per cui i dati personali sono trattati, ove possibile al periodo in cui i dati personali sono trattati, ai destinatari dei dati personali, alla logica cui risponde qualsiasi trattamento automatizzato dei dati e, almeno quando è basato sulla profilazione, alle possibili conseguenze di tale trattamento. Ove possibile, il titolare del trattamento dovrebbe poter fornire l'accesso remoto a un sistema sicuro che consenta all'interessato di consultare direttamente i propri dati personali. Tale diritto non dovrebbe ledere i diritti e le

libertà altrui, compreso il segreto industriale e aziendale e la proprietà intellettuale, segnatamente i diritti d'autore che tutelano il software. Tuttavia, tali considerazioni non dovrebbero condurre a un diniego a fornire all'interessato tutte le informazioni. Se il titolare del trattamento tratta una notevole quantità d'informazioni riguardanti l'interessato, il titolare in questione dovrebbe poter richiedere che l'interessato precisi, prima che siano fornite le informazioni, l'informazione o le attività di trattamento cui la richiesta si riferisce".

***iii*) diritto di rettifica e diritto alla cancellazione dei dati (e c.d. diritto all'oblio)**

Si tratta di diritti disciplinati, rispettivamente, dagli artt. 16 e 17. Il diritto di rettifica prevede la correzione di dati personali inesatti, nonché il diritto di ottenere l'integrazione dei dati personali incompleti. Il Considerando 65 del Regolamento verte sia sul diritto alla rettifica dei dati sia su quello alla loro cancellazione, entrambi collegati al diritto alla corretta e diacronica rappresentazione dell'individuo, anche in ambito digitale. Ad ogni modo, il c.d. diritto all'oblio [26] (che parte della dottrina [27] distingue dal diritto alla cancellazione e talaltra [28], invece, lo include in essa) costituisce una delle novità di maggiore rilievo introdotte dal GDPR. Alla stregua dell'art. 17, nonché dei Considerando 65, 66 e 156, l'interessato può chiedere che i propri dati personali siano cancellati e non più suscettibili di trattamento, qualora non necessari alle finalità per le quali sono stati raccolti. La richiesta di cancellazione riguarda, altresì, le ipotesi di trattamenti illeciti, di revoca del consenso (in assenza di altra base giuridica), di esercizio del diritto di opposizione (su cui si v. *infra*), di adempimento dell'obbligo legale o quando i dati personali sono stati raccolti relativamente all'offerta di servizi della società dell'informazione. Il par. 2 dell'art. 17 specifica che "Il titolare del trattamento, se ha reso pubblici dati personali ed è obbligato, ai sensi del paragrafo 1, a cancellarli, tenendo conto della tecnologia disponibile e dei costi di attuazione adotta le misure ragionevoli, anche tecniche, per informare i titolari del trattamento che stanno trattando i dati personali della richiesta dell'interessato di cancellare qualsiasi link, copia o riproduzione dei suoi dati personali".

La previsione del diritto alla cancellazione/oblio rappresenta, dunque, l'approdo normativo del lungo dibattito dottrinale e giurisprudenziale (si pensi al "diritto alla deindicizzazione", per come elaborato dalla sentenza della Corte di Giustizia del 13 maggio 2014, causa C-131/12, c.d. "Google Spain", [29] in *Foro it*., 2014, IV, 295, con nota di R. Pardolesi e A. Palmieri). Il legislatore eurounirario ha positivizzato il "nuovo" diritto, garantendo un bilanciamento tra istanze differenti, come dimostrano le deroghe previste dal paragrafo 3 del citato art. 17. Il diritto alla cancellazione/oblio non opera, infatti, nel caso in cui il trattamento è necessario per: l'esercizio della libertà di espressione e di informazione; l'adempimento di un obbligo legale; i motivi di interesse pubblico nel settore della sanità; l'esercizio o difesa di un diritto in sede giudiziaria ovvero – per quanto rileva ai nostri scopi – il perseguimento di fini di archiviazione, di pubblico interesse, di ricerca scientifica, storica o fini statistici "conformemente all'articolo 89, paragrafo 1, nella misura in cui il diritto (…) rischi di rendere impossibile o di pregiudicare gravemente il conseguimento degli obiettivi di tale trattamento".

Invero, l'art. 17, nonostante sia rubricato "Diritto alla cancellazione", con l'ulteriore inciso "diritto all'oblio", nella sua formulazione testuale non contiene riferimenti al "*right to be forgotten*", così da alimentare dubbi sull'effettiva portata di quest'ultimo diritto.

iv) diritto di limitazione del trattamento

L'esatta individuazione di tale diritto, previsto dall'art. 18 GDPR, presuppone la nozione di limitazione che, ai sensi dell'art. 4, n. 3, del Regolamento, costituisce "il contrassegno dei dati personali conservati con l'obiettivo di limitarne il trattamento in futuro". Questa disposizione dovrebbe essere tenuta in debita considerazione soprattutto da chi si occupa di programmazione e di sviluppo dei sistemi informativi, affinché gli stessi siano connotati da una funzionalità che consenta, per l'appunto, di "contrassegnare" i dati personali memorizzati, e la loro (potenziale) limitazione, in qualunque momento, da parte dell'interessato o dell'Autorità Garante. Si tratta, dunque, di sospensione temporanea (ma che può anche diventare

permanente) del trattamento in corso. Tale diritto è esercitabile solo al ricorrere di almeno una delle seguenti ipotesi: 1. l'interessato contesta l'esattezza dei dati personali; 2. il trattamento è illecito e l'interessato si oppone alla cancellazione dei dati personali; 3. i dati sono necessari all'interessato per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria; 4. l'interessato si è opposto al trattamento e si è in attesa delle verifiche necessarie per determinare se i motivi legittimi del titolare del trattamento prevalgano su quelli dell'interessato. In ciascuno di questi casi, quindi, i dati possono essere trattati soltanto ai fini della loro conservazione, a meno che non vi sia il consenso dell'interessato o il trattamento sia necessario per "l'esercizio o la difesa di un diritto in sede giudiziaria oppure per tutelare i diritti di un'altra persona fisica o giuridica o per motivi di interesse pubblico rilevante dell'Unione Europea o di uno Stato Membro" (art. 18, par. 2, GDPR). Nel caso in cui i dati personali oggetto di limitazione siano stati comunicati ad altri soggetti, è onere del titolare del trattamento darne comunicazione a ciascuno dei destinatari, a meno che ciò sia impossibile o implichi uno sforzo sproporzionato (art. 19 GDPR). Il Considerando n. 67 esemplifica le modalità per limitare il trattamento, attraverso il trasferimento temporaneo di dati selezionati verso un altro sistema operativo o tramite rimozione temporanea dei dati pubblicati da un sito web. Lo stesso *Considerando* evidenzia, inoltre, che "Negli archivi automatizzati, la limitazione del trattamento dei dati personali dovrebbe, in linea di massima, essere assicurata mediante dispositivi tecnici in modo tale che i dati personali non siano sottoposti a ulteriori trattamenti e non possano più essere modificati. Il sistema dovrebbe indicare chiaramente che il trattamento dei dati personali è stato limitato".

v) diritto di notificazione

Tale diritto è previsto dall'art. 19 del GDPR, che costituisce una disposizione "di chiusura", in virtù della quale il titolare del trattamento comunica a ciascuno dei destinatari cui sono stati trasmessi i dati personali le eventuali rettifiche o cancellazioni o limitazioni del trattamento, effettuate a norma dell'art. 16, dell'art. 17, paragrafo 1 e dell'art. 18, GDPR, salvo che ciò si riveli impossibile o implichi uno sforzo sproporzionato. Il titolare del trattamento comunica all'interessato le predette informazioni qualora questi lo richieda espressamente.

vi) diritto alla portabilità dei dati

Tale diritto, previsto dall'art. 20 GDPR, è da annoverare fra i "nuovi" diritti riconosciuti all'interessato nel Capo III e rappresenta una concreta esplicazione delle garanzie previste dal Regolamento sia rispetto all'effettiva circolazione dei dati sia riguardo al controllo sul flusso delle informazioni.

La portabilità consente, infatti, all'interessato di "ricevere in un formato strutturato, di uso comune e leggibile da dispositivo automatico i dati personali che lo riguardano forniti a un titolare del trattamento e ha il diritto di trasmettere tali dati a un altro titolare del trattamento senza impedimenti da parte del titolare del trattamento cui li ha forniti".

Da un punto di vista operativo, il diritto *de quo* permette agli interessati di ottenere i dati personali forniti al titolare del trattamento, in un formato di uso comune (per es., un supporto personale o un *cloud* privato) strutturato, leggibile meccanicamente, al fine di trasmetterli a un diverso titolare. Il diritto alla portabilità può essere esercitato, per esempio, per ottenere la restituzione di dati personali resi a un'azienda o a un fornitore di servizi on line, allo scopo di trasmetterli ad uno diverso (*social network*, fornitori di servizi di rete, ecc.).

La fattispecie disciplinata dall'art. 20 riguarda soltanto trattamenti basati sul consenso (ai sensi dell'art. 6, par. 1, lett. *a* o ai sensi dell'art. 9, par. 2, lett. *a*, GDPR, in caso di dati particolari) o necessari all'esecuzione di un contratto di cui è parte l'interessato (ai sensi dell'art. 6, par. 1, lett. b, GDPR) e operanti con modalità automatizzate, anche solo parzialmente. La previsione conferma l'intento del Legislatore eurounitario di promuovere non solo il potenziamento della tutela "statica" dei dati personali, ma anche lo sviluppo dell'economia digitale, attraverso l'utilizzo di formati interoperabili da parte dei titolari, così da consentire la

portabilità dei dati. Occorre evidenziare, inoltre, che il diritto alla portabilità è escluso, qualora il trattamento sia necessario all'adempimento di funzioni pubbliche, "per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento" (così l'art. 20, par. 3, seconda parte, GDPR). Il Considerando n. 68 del Regolamento specifica che l'esercizio di tale diritto non opera nei seguenti casi: 1. nei confronti dei titolari del trattamento che effettuano operazioni sui dati personali nell'esercizio delle loro pubbliche funzioni; 2. per l'adempimento di un obbligo legale e di un compito svolto nel pubblico interesse; 3. nell'esercizio di pubblici poteri di cui è investito il titolare del trattamento.

L'art. 20, par. 3, GDPR afferma, inoltre, che il diritto alla portabilità dei dati lascia impregiudicato il diritto alla loro cancellazione e, al par. 4, che "non deve ledere i diritti e le libertà altrui".

Il diritto, *ex* art. 20, GDPR, di cui i titolari del trattamento devono informare gli interessati non risponde solo all'esigenza di potenziare il controllo dei singoli sui dati personali che li riguardano, garantendo loro un ruolo "attivo" nel trattamento, ma anche allo scopo di agevolare la libera circolazione delle informazioni nell'economia digitale. Tale diritto promuove, dunque, la concorrenza tra le aziende, l'innovazione e lo sviluppo di nuovi servizi ed evita che l'interessato debba fornire di nuovo i suoi dati al nuovo titolare. Il diritto alla portabilità risponde, dunque, alla libera circolazione delle informazioni, nonché, più in generale, allo sviluppo e al consolidamento dei servizi della società dell'informazione.

vii) diritto di opposizione

L'esercizio di tale diritto, previsto dall'art. 21 GDPR, obbliga il titolare a interrompere il trattamento dei dati. A questo riguardo, pare opportuno sottolineare che l'interessato può opporsi, in qualsiasi momento, "per motivi connessi alla sua situazione particolare, al trattamento dei dati personali che lo riguardano ai sensi dell'articolo 6, paragrafo 1, lettere e) o f), compresa la profilazione (…)". Il *data controller*, che intenda proseguire il trattamento, ha un onere di giustificazione ulteriore, che consiste nella prova della sussistenza di motivi cogenti prevalenti o della sussistenza di esigenze di tutela, connesse a un diritto da accertare, esercitare e difendere in giudizio.

Il diritto di opposizione rappresenta, dunque, insieme agli altri diritti della prima parte del Capo III, una forma di tutela dell'interesse specifico del *data subject* a non subire un trattamento dei propri dati, che reputi dannoso o illegittimo.

viii) diritto a non subire profilazioni inconsapevoli

tale diritto, previsto dall'art. 22 del GDPR, trova fondamento nel dibattito dovuto all'emersione del ricorso ad algoritmi di decisione automatizzata, tenuto anche conto della gravità degli effetti che, talvolta, queste soluzioni tecniche possono avere sui destinatari [30]. A tale riguardo, il legislatore eurounitario sembra aver assunto una posizione cauta, positivizzata nell'art. 22 del GDPR, ai sensi del quale "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". Ad ogni modo, lo stesso Regolamento prevede ipotesi in deroga assai significative. La disposizione appena citata non si applica, infatti, quando la decisione si basa sul consenso esplicito dell'interessato; è necessaria per la conclusione o l'esecuzione di un contratto tra l'interessato e il titolare del trattamento; è autorizzata dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento (purchè tendenzialmente non riguardi dati particolari, come previsto dall'art. 22, par. 4). Nei casi in cui la profilazione si basi sul consenso o sul contratto, il titolare del trattamento attua misure appropriate per tutelare i diritti, le libertà e i legittimi interessi dell'interessato, "garantendo il diritto di ottenere l'intervento umano da parte del titolare del trattamento, di esprimere la propria opinione e di contestare la decisione".

Al riguardo, pare opportuno evidenziare che il 3 novembre 2021 il Comitato dei Ministri del Consiglio d'Europa ha adottato la raccomandazione sulla protezione degli individui con riguardo ai trattamenti automatizzati dei dati personali nell'ambito della profilazione (27CM/Rec(2021)18, CM–Profiling) di aggiornamento di una precedente raccomandazione adottata nel 2010 (CM/Rec(2010)13) in realtà afferente a una tematica diversa.

A protezione dei dati personali in caso di profilazione, gli Stati devono avvalersi di sistemi rispettosi della *privacy* sin dalla fase di progettazione (*privacy by design*), evitare errori e garantire il diritto dell'interessato a ottenere, in tempi ragionevoli, le informazioni che lo riguardano. La sezione B è dedicata alle operazioni di profilazione svolte da *public authorities*, tenute a rispettare i diritti fondamentali, come interpretati dalla Corte europea dei diritti dell'uomo.

Dall'esame del Capo III fin qui condotto, si evince certamente che il *data subject* è una parte attiva delle procedure e delle operazioni di trattamento effettuate sui propri dati personali. Il GDPR gli attribuisce un ampio potere di controllo e di intervento, che si declina in specifiche prerogative finalizzate a garantire il rispetto dei diritti in un mercato aperto alla circolazione, anche transfrontaliera, delle persone e delle loro informazioni e dunque a conciliare la libertà di trattare i dati con il limite rappresentato dalla effettività dei diritti spettanti all'interessato.

2.5 5° step: verificare se occorre una valutazione di impatto

La valutazione di impatto (*Data protection Impact Assessment* o DPIA) [31] è uno degli adempimenti di maggiore rilievo previsti nel nuovo quadro normativo.

Si tratta, infatti, di una manifestazione del principio di responsabilizzazione (*accountability*), più volte citato, che impone ai titolari non solo di osservare le disposizioni in tema di *privacy*, ma anche di dimostrarne il rispetto.

Il GDPR obbliga, infatti, il titolare a effettuare la valutazione di impatto in caso di trattamenti a rischio elevato per i diritti e le libertà degli interessati, prima di darvi inizio. È possibile, inoltre, consultare l´autorità di controllo nell'ipotesi in cui le misure tecniche e organizzative individuate dal *data controller* per mitigare l´impatto del trattamento non siano ritenute sufficienti, ossia quando il rischio residuale per i diritti e le libertà degli interessati resti elevato.

Ai sensi dell'art. 35 GDPR, il trattamento, che prevede l'uso di particolari tecnologie, può comportare un rischio elevato per i diritti e le libertà delle persone interessate a causa del monitoraggio sistematico dei loro comportamenti (ossia in caso di trattamento automatizzato, inclusa la profilazione) o per il gran numero degli interessati (c.d. trattamento su larga scala) oppure per il trattamento di dati sensibili o per una combinazione di questi e altri fattori.

L'art. 35, par. 3, specifica che la valutazione d'impatto è richiesta, in particolare, nei casi seguenti:

"a) una valutazione sistematica e globale di aspetti personali relativi a persone fisiche, basata su un trattamento automatizzato, compresa la profilazione, e sulla quale si fondano decisioni che hanno effetti giuridici o incidono in modo analogo significativamente su dette persone fisiche;

b) il trattamento, su larga scala, di categorie particolari di dati personali di cui all'articolo 9, paragrafo 1, o di dati relativi a condanne penali e a reati di cui all'articolo 10; o

c) la sorveglianza sistematica su larga scala di una zona accessibile al pubblico".

A tale riguardo, si rinvia alla consultazione dello schema elaborato dal Garante della Privacy, di ausilio per comprendere quando è necessario effettuare la DPIA [32].

Il citato art. 35, al par. 7, prevede il contenuto minimo della DPIA, che consiste in:

"a) una descrizione sistematica dei trattamenti previsti e delle finalità del trattamento, compreso, ove applicabile, l'interesse legittimo perseguito dal titolare del trattamento;

b) una valutazione della necessità e proporzionalità dei trattamenti in relazione alle finalità;

c) una valutazione dei rischi per i diritti e le libertà degli interessati di cui al paragrafo 1; e

d) le misure previste per affrontare i rischi, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformità al presente regolamento, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione".

Sul punto, il *Working party* 29 ha fornito delle linee-guida [33] che chiariscono quando una valutazione di impatto è obbligatoria (oltre ai casi espressamente indicati dall'art. 35 GDPR), chi è tenuto a porla in essere (ossia il titolare, coadiuvato dal responsabile della protezione dei dati, se designato), di cosa consta (attraverso alcuni esempi) e la necessità di considerarla non come un adempimento *una tantum*, ma come un'operazione da sottoporre ad aggiornamento costante [34].

Ai fini della presente ricerca, in considerazione dei trattamenti di cui si è già dato conto, seppur sinteticamente, (e che saranno approfonditi nei casi di studio, *infra*) la valutazione d'impatto è fortemente consigliata per ciascuno di essi.

All'esito della valutazione di impatto, il titolare può decidere se iniziare il trattamento (previa adozione delle misure in grado di mitigare sufficientemente il rischio) o consultare l'autorità di controllo per ricevere indicazioni sulle eventuali misure necessarie per gestire il rischio residuale. Ai sensi dell'art. 58 GDPR, ove necessario, l'Autorità garante può adottare tutte le misure correttive: dall'ammonimento del titolare fino alla limitazione o al divieto di procedere al trattamento.

2.6 6° step: adottare le misure di sicurezza opportune

Come evidenziato, la DPIA deve specificare anche le misure di sicurezza in grado di "garantire un livello di sicurezza adeguato al rischio" del trattamento (art. 32, par. 1, GDPR). Tale disposizione prevede un elenco non esaustivo delle misure tecniche e organizzative che il titolare deve mettere in atto per evitare violazioni della disciplina sulla privacy.

L'art. 32 menziona, tra le misure tecniche, la pseudonimizzazione (su cui si v. *supra*) e la cifratura dei dati personali. Per quanto riguarda le misure organizzative, la disposizione include la capacità di garantire, 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 incidenti sia fisici sia tecnici (si pensi, ad es., alla predisposizione di procedure di *back-up* per il recupero e il ripristino di dati); la procedura per testare, verificare e valutare regolarmente l'efficacia delle misure per la sicurezza del trattamento.

In conformità con l'approccio "*risk based*" del Regolamento, tali misure devono essere adottate tenuto 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".

Occorre segnalare, inoltre, l'art. 32, par. 4, GDPR, che impone, come ulteriore accorgimento, la formazione dei soggetti autorizzati al trattamento dei dati. Al contempo, l'art. 25 GDPR circoscrive "l'accessibilità" al trattamento (si pensi, ad es., alla necessità di una procedura di autenticazione e di corretta gestione delle password, "forti", individuali e da cambiare nel corso del tempo, oltre all'accesso limitato a una singola banca dati/*directory* a seconda delle mansioni svolte).

Si segnala, inoltre, l'opportunità di individuare un referente per la gestione della sicurezza e di eventuali incidenti.

2.7 7° step: notazioni in caso di trasferimenti di dati verso Stati terzi

Il trasferimento di dati personali verso Paesi situati al di fuori dell'Unione Europea o verso organizzazioni internazionali è consentito solo alle condizioni previste dagli artt. 45, 46 e 47 del Regolamento.

Occorre evidenziare che i trasferimenti di dati verso Stati terzi ritenuti "adeguati", sulla base della decisione assunta dalla Commissione europea (art. 45 GDPR) o di apposite garanzie (art. 46), come le clausole contrattuali modello, debitamente adottate o le norme vincolanti d'impresa (approvate ai sensi dell'art. 47 del Regolamento), o di specifiche deroghe, non richiedono l'autorizzazione nazionale del Garante. Tale autorizzazione occorre, invece, quando un titolare intende utilizzare clausole contrattuali non riconosciute come adeguate tramite decisione della Commissione europea o accordi amministrativi stipulati tra autorità pubbliche.

Al riguardo, si evidenzia che il 4 giugno 2021, la Commissione europea ha adottato le Clausole Contrattuali Standard (SCC, *Standard Contractual Clauses*). Si tratta di misure contrattuali che vincolano l'importatore a un'adeguata protezione dei dati ricevuti. Le SCC costituiscono, dunque, uno degli strumenti indispensabili per consentire il trasferimento di dati personali da un Paese – come il nostro – sottoposto agli stringenti obblighi il GDPR a uno che non garantisce un adeguato livello di protezione dei dati personali.

L'autorizzazione al trasferimento da parte del Garante occorre, invece, in caso di impegni sottoscritti tramite l'adesione al codice di condotta o allo schema di certificazione.

Il trasferimento a Stati terzi basato sulle sentenze o decisioni amministrative emesse da autorità di tale Paese terzo è tendenzialmente vietato (art. 48 GDPR).

Ai sensi dell'art. 49 del GDPR "In mancanza di una decisione di adeguatezza ai sensi dell'articolo 45, paragrafo 3, o di garanzie adeguate ai sensi dell'articolo 46, comprese le norme vincolanti d'impresa, è ammesso il trasferimento o un complesso di trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale soltanto se si verifica una delle seguenti condizioni:

a) l'interessato abbia esplicitamente acconsentito al trasferimento proposto, dopo essere stato informato dei possibili rischi di siffatti trasferimenti per l'interessato, dovuti alla mancanza di una decisione di adeguatezza e di garanzie adeguate;

b) il trasferimento sia necessario all'esecuzione di un contratto concluso tra l'interessato e il titolare del trattamento ovvero all'esecuzione di misure precontrattuali adottate su istanza dell'interessato;

c) il trasferimento sia necessario per la conclusione o l'esecuzione di un contratto stipulato tra il titolare del trattamento e un'altra persona fisica o giuridica a favore dell'interessato;

d) il trasferimento sia necessario per importanti motivi di interesse pubblico;

e) il trasferimento sia necessario per accertare, esercitare o difendere un diritto in sede giudiziaria;

f) il trasferimento sia necessario per tutelare gli interessi vitali dell'interessato o di altre persone, qualora l'interessato si trovi nell'incapacità fisica o giuridica di prestare il proprio consenso;

g) il trasferimento sia effettuato a partire da un registro che, a norma del diritto dell'Unione o degli Stati membri, mira a fornire informazioni al pubblico e può esser consultato tanto dal pubblico in generale quanto da chiunque sia in grado di dimostrare un legittimo interesse, solo a condizione che sussistano i requisiti per la consultazione previsti dal diritto dell'Unione o degli Stati membri.

Se non è possibile basare il trasferimento su una disposizione dell'articolo 45 o 46, comprese le disposizioni sulle norme vincolanti d'impresa, e nessuna delle deroghe in specifiche situazioni a norma del primo comma del presente paragrafo è applicabile, il trasferimento verso un paese terzo o un'organizzazione internazionale sia ammesso soltanto se non è ripetitivo, riguarda un numero limitato di interessati, è necessario per il perseguimento degli interessi legittimi cogenti del titolare del trattamento, su cui non prevalgano gli interessi o i diritti e le libertà dell'interessato, e qualora il titolare e del trattamento abbia valutato tutte le circostanze relative al trasferimento e sulla base di tale valutazione abbia fornito garanzie adeguate relativamente alla protezione dei dati personali. Il titolare del trattamento informa del trasferimento l'autorità di controllo. In

aggiunta alla fornitura di informazioni di cui agli articoli 13 e 14, il titolare del trattamento informa l'interessato del trasferimento e degli interessi legittimi cogenti perseguiti".

2.8 *Focus sul rapporto tra privacy e nuove tecnologie: la* data protection *in caso di* smart meters*, piattaforme,* blockchain *e* smart contracts

Tra gli strumenti per la gestione intelligente dei consumi energetici degli immobili**,** utilizzati nel progetto e, più in generale, nelle sperimentazioni , vi è l'impiego di ***smart meters*** (ossia di contatori "intelligenti"), a loro volta, indispensabili per la costruzione di ***smart grid*** (ossia di reti "intelligenti"). Tramite gli *smart meters* è possibile la lettura del consumo energetico dell'edificio e la trasmissione dei dati raccolti al di fuori dell'immobile.

I dati generati da contatori intelligenti sono associati a elementi identificativi univoci, come quello del contatore. In caso di utenze domestiche tale elemento identificativo è collegato al soggetto responsabile della fattura. Ai nostri fini, occorre specificare che ENEA non instaura un rapporto di fornitore o venditore, quindi, non ha un codice *point of delivery* (POD) dell'utenza, a differenza del *Distribution System Operator* (DSO), che è, per l'appunto, il responsabile della fattura.

Al contempo, tramite i dati raccolti con la misurazione intelligente dei consumi, è possibile profilare il consumatore, con riferimento all'utilizzo di energia, e adottare decisioni che lo riguardano direttamente, perché in grado di incidere sui suoi comportamenti.

Per tale ragione, già con la Raccomandazione 2012/148/UE, la Commissione europea contiene diverse indicazioni in tema di sicurezza dei dati, partendo dal principio di "*data protection by design*" (punti 24-28) e afferma che "La frequenza generalmente ammessa come necessaria per l'aggiornamento dei dati è almeno ogni 15 minuti. Le comunicazioni diventeranno probabilmente più rapide con l'evoluzione tecnica e lo sviluppo di nuovi servizi energetici".

Di recente, a proposito dei sistemi di misurazione intelligente, il considerando 57 della citata Direttiva 2018/944 ha sottolineato che "È importante che gli Stati membri, a prescindere dal modello di gestione dei dati, introducano regole trasparenti che stabiliscano condizioni non discriminatorie di fruizione e assicurino il massimo livello di cibersicurezza e protezione dei dati, nonché l'imparzialità degli enti che trattano i dati". Il considerando 91 specifica, inoltre, che l'interpretazione e applicazione della Direttiva stessa deve avvenire in conformità della disciplina sulla privacy. L'art. 19 ribadisce la necessità di rispettare la disciplina sulla privacy con specifico riferimento ai sistemi di gestione dell'energia dei consumatori e reti intelligenti.

In particolare, l'art. 20 stabilisce, alla lett. a), che "I dati sui consumi storici convalidati sono resi accessibili e visualizzabili facilmente e in modo sicuro ai clienti finali, su richiesta e senza costi aggiuntivi. I dati sui consumi in tempo quasi reale non convalidati sono anch'essi resi accessibili facilmente e in modo sicuro ai clienti finali, senza costi aggiuntivi e attraverso un'interfaccia standardizzata o mediante l'accesso a distanza, a sostegno dei programmi di efficienza energetica automatizzata, della gestione della domanda e di altri servizi" e, alla lett. b), che "la sicurezza dei sistemi di misurazione intelligenti e della comunicazione dei dati è conforme alla pertinente normativa dell'Unione in materia di sicurezza, tenendo debitamente conto delle migliori tecniche disponibili per garantire il più alto livello di cibersicurezza tenendo al contempo presenti i costi e il principio di proporzionalità".

L'art. 20, lett. c), ricorda nuovamente la necessità di rispettare la normativa dell'Unione sulla protezione dei dati e della vita privata e la lett. f) stabilisce un diritto all'informazione del cliente, prima o al momento dell'installazione del contatore intelligente, "riguardo al pieno potenziale del dispositivo in termini di gestione della lettura e di monitoraggio del consumo di energia elettrica, nonché riguardo alla raccolta e al trattamento dei dati personali (…)". Resta fermo, inoltre, il diritto alla portabilità dei dati misurati dal contatore da parte del cliente finale, che può recuperarli o trasmetterli a terzi senza costi aggiuntivi.

A tale riguardo, pare opportuno ricordare quanto indicato dall'art. 23, dedicato alla "Gestione dei dati": "1. Al momento di stabilire le regole per la gestione e lo scambio dei dati, gli Stati membri o, qualora lo Stato membro abbia così disposto, l'autorità competente designata indicano le norme relative all'accesso ai dati del cliente finale da parte dei soggetti ammessi in conformità del presente articolo e del quadro giuridico dell'Unione applicabile. Ai fini della presente direttiva, si considera che i dati comprendano quelli di misurazione e di consumo nonché i dati richiesti per cambiare fornitore e per la gestione della domanda e altri servizi

2. Gli Stati membri organizzano la gestione dei dati in modo tale che l'accesso ai dati e lo scambio degli stessi sia efficiente e sicuro, garantendo altresì la protezione e la sicurezza dei dati. Indipendentemente dal modello utilizzato per la gestione dei dati in uno Stato membro, i soggetti responsabili della gestione dei dati forniscono a qualsiasi soggetto ammesso l'accesso ai dati del cliente finale conformemente al paragrafo 1. I dati richiesti devono essere messi a disposizione dei soggetti ammessi in modo non discriminatorio e simultaneo. L'accesso ai dati deve essere facile e le relative procedure attinenti devono essere pubblicamente disponibili.

Fatti salvi i compiti dei responsabili della protezione dei dati a norma del regolamento (UE) n. 2016/679, gli Stati membri hanno la facoltà di richiedere ai soggetti responsabili della gestione dei dati la designazione di un responsabile della conformità, incaricato di controllare l'attuazione delle misure adottate da tali soggetti per assicurare un accesso non discriminatorio ai dati e la conformità ai requisiti della presente direttiva. (…)

5. Ai clienti finali non è addebitato alcun costo supplementare per l'accesso ai loro dati o per la richiesta di mettere tali dati a disposizione".

Con riferimento alla *compliance* dei sistemi "intelligenti" di misurazione dell'energia al GDPR, occorre evidenziare poi che il *Working Party Art. 29* ha attenzionato le problematiche relative, in generale, all'impiego di *IoT*, nel parere n. 8 del 2014, nel parere n. 8 del 2014 (*Recent Developments on the Internet of Things*), fornendo una serie di raccomandazioni, anche pratiche, agli operatori del settore.

Ai fini che qui rilevano si segnala il parere *Working Party Art. 29* del 4 aprile 2011, n. 12, proprio sui contatori intelligenti (*smart metering*).

In tale occasione, oltre a individuare, con elenco non esaustivo (di cui si è già dato conto *supra*), i possibili dati personali trattati con *smart meters*, il Gruppo di lavoro ha chiarito che l'uso di tali strumenti comporta il coinvolgimento di numerosi soggetti, quali i fornitori di energia, i gestori della rete energetica, gli enti di regolamentazione e quelli governativi, i fornitori terzi di servizi e gli operatori nel settore delle comunicazioni.

La vastità e la complessità di rapporti rendono necessaria un'analisi casistica per l'individuazione dei singoli ruoli ricoperti da tali soggetti nell'ambito del trattamento.

Sul tema, le questioni più rilevanti che, secondo il Gruppo di lavoro, meritano considerazione riguardano:

i) la tutela della vita privata fin dalla progettazione ("*Privacy by design*"), non solo tramite misure di sicurezza, ma anche con la minimizzazione dei dati personali oggetto di trattamento. Ciò comporta, innanzitutto, che la frequenza di letture sia ridotta a quanto necessario per il funzionamento del sistema.

"Le specifiche tecniche della rete dovrebbero altresì garantire che i dati raccolti rimangano all'interno della rete domestica, salvo che la trasmissione degli stessi altrove sia necessaria o che l'interessato acconsenta alla trasmissione".

L'obiettivo dovrebbe essere quello di trattare il minore quantitativo possibile di dati e di affidare tale compito solo a soggetti competenti e nei limiti di quanto indispensabile per lo svolgimento delle loro funzioni.

ii) l'esigenza di garantire i dritti individuali (già indicati *supra*) e di fornire informazioni adeguate agli interessati, affinchè comprendano le implicazioni del trattamento e siano in grado di conoscere, in modo esauriente, l'impiego dei loro dati.

Il *Working Party* Art. 29 evidenzia, tra l'altro, l'importanza della "possibilità di garantire che gli interessati siano nelle condizioni di esercitare i loro diritti in tutta facilità utilizzando strumenti che consentono loro di accedere direttamente ai dati".

iii) l'adozione di misure tecniche e organizzative per:

"prevenzione della comunicazione non autorizzata di dati personali;

mantenimento dell'integrità dei dati per impedirne la modifica non autorizzata;

verifica effettiva dell'identità di eventuali destinatari di dati personali;

occorre evitare che importanti servizi siano interrotti a causa di attacchi alla sicurezza dei dati personali;

strutture per effettuare controlli adeguati dei dati personali conservati o trasmessi da un contatore;

controlli dell'accesso adeguati e periodi opportuni di conservazione;

aggregazione di dati quando non sono richiesti dati di rilevanza individuale".

Si segnala, inoltre, che, sul sito dell'Unione europea [35], risulta pubblicato un modello *ad hoc* di valutazione dell'impatto sulla protezione dei dati (su cui si rinvia *supra*) per le reti intelligenti e per l'ambiente di misurazione intelligente.

Si tratta di un prototipo di DPIA che, seppur non obbligatorio, è rivolto specificatamente ai soggetti che operano tramite *smart grid*, come i gestori di sistemi di distribuzione, i generatori, i fornitori, gli operatori e le società di servizi energetici

Il modello fornisce esempi di misure di controllo per la *compliance* al GDPR delle *smart grid* fin dall'inizio della loro progettazione. "Inoltre, i responsabili del trattamento dei dati che utilizzano il modello DPIA possono godere di un vantaggio competitivo fornendo fiducia e guadagnando reputazione per il loro impegno nella protezione dei dati personali".

Nel capitolo 1 del documento è illustrato il contesto necessario per comprendere il processo della DPIA nell'ambito delle reti intelligenti, le condizioni legali e commerciali e la relativa terminologia. Il capitolo 2 contiene una guida esplicativa e il capitolo 3 un questionario-modello.

I nuovi modelli presuppongono, inoltre, trattamenti dei dati personali tramite **piattaforme** che siano conforme ai principi e alle regole in tema di privacy.

La progettazione di tali soluzioni informatiche richiede, dunque, la massima sicurezza delle attività compiute; documentazione e gestione degli accessi (non generici) degli utenti, degli *assets*, delle operazioni compiute sul database in lettura o in modifica, della *data retention*, dei *file log*, delle terze parti, della comunicazione delle informazioni e dei dati preferibilmente pseudonimizzati e/o crittografati [36]

Si tratta di aspetti in gran parte attenzionati anche dal Garante della Privacy in occasione del provvedimento su *data breach*, del 4 aprile 2019, n. 83, con cui l'Autorità ha sanzionato la piattaforma *Rosseau*.

In tale atto, oltre al "mancato, completo tracciamento degli accessi al database del sistema *Rousseau* e delle operazioni sullo stesso compiute (…)", il Garante ha evidenziato che la condivisione delle credenziali di autenticazione da parte di più incaricati impedisce di attribuire le azioni compiute in un sistema informatico, "con pregiudizio anche per il titolare, privato della possibilità di controllare l'operato di figure tecniche così rilevanti". Al contempo, in contrasto con la disciplina in tema di privacy, tramite la condivisione delle credenziali e in assenza di una specifica volontà del titolare o del responsabile, un soggetto autorizzato soltanto all'uso di una determinata piattaforma finirebbe per poter operare anche su altre che sfruttino il medesimo sistema di autenticazione.

Per completezza, pare opportuno segnalare che, con la Determinazione n. 529/2021, l'Agenzia per l'Italia digitale (AGID), in collaborazione con l'Ufficio legislativo del Ministro per l'innovazione e la transizione al digitale e con il supporto del Dipartimento per la trasformazione digitale, ha adottato le Linee guida dell'Indice nazionale dei domicili digitali delle persone fisiche, dei professionisti e degli altri enti di diritto privato non tenuti all'iscrizione in albi, elenchi o registri professionali o nel registro delle imprese (INAD), di cui all'art. 6-*quater* del Codice dell'Amministrazione Digitale (CAD). Nel novero di tali soggetti, vi è – ad esempio – l'amministratore di condominio.

Per domicilio digitale si intende l'indirizzo elettronico eletto presso un servizio di posta elettronica certificata (PEC) o un servizio elettronico di recapito certificato qualificato, come definito dal Regolamento eIDAS, valido per le comunicazioni elettroniche con valore legale, ai sensi dell'articolo 1, comma 1, lett. n-*ter* del CAD.

Si ricorda, inoltre, che, a partire dal 1° ottobre 2021, a seguito delle novità introdotte dalla legge 11 settembre 2020, n.120, che ha reso efficaci le disposizioni del decreto "Semplificazione e innovazione digitale", tutti i servizi digitali della p.A. devono essere accessibili ai cittadini tramite l'autenticazione con Sistema Pubblico d'Identità Digitale (SPID) o Carta d'Identità Elettronica (CIE) o la Carta Nazionale dei Servizi (CNS).

Come più volte evidenziato, le sperimentazioni sui nuovi modelli di produzione e distribuzione dell'energia possono comportare l'utilizzo della ***blockchain*** e la remunerazione del comportamento virtuoso degli utenti e/o dei partecipanti alla comunità, attraverso ***smart contract*** (contratto o, meglio, strumento di negoziazione "intelligente") e *token* (o *assets* digitali/valute complementari).

Gli *smart contracts* (e il conseguente flusso di *token*, spostati da un "*wallet*" a un altro) possono prescindere dalla "catena di blocchi", ma – come nel progetto in essere – spesso sono concepiti all'interno di una *blockchain*, perchè solo le caratteristiche di quest'ultima ne garantiscono l'immodificabilità e l'esecuzione automatica del codice informatico [37].

La *blockchain* funziona tramite un algoritmo altamente performante e rientra nel novero delle tecnologie di *Distributed Ledger*, ossia sistemi basati sul registro distribuito, condiviso tra più partecipanti, costituito da una sequenza di blocchi di dati, oltre che leggibile e modificabile da più nodi di una rete. Tramite questa tecnologia, transazioni fra blocchi di dati vengono archiviate in modo distribuito agganciate a blocchi precedenti, per garantirne la loro inalterabilità. In assenza del controllo e dalla regolazione da parte delle autorità centralizzate, per validare le modifiche apportate registro (e, dunque, per concatenare un blocco all'altro), i nodi devono raggiungere il consenso di chi partecipa alla rete.

Di conseguenza, le caratteristiche principali della *blockchain* sono:

i) la tracciabilità/verificabilità, perché i trasferimenti su registro sono tracciati in toto e verificabili;

ii) la decentralizzazione, perchè la registrazione delle informazioni avviene con distribuzione su più nodi;

iii) la disintermediazione, perchè consente trasferimenti *peer-to-peer* di risorse senza enti centrali fidati come intermediari;

iv) la tendenziale immutabilità, perchè i dati iscritti del registro non possono essere modificati senza il consenso della rete e

v) la sicurezza dovuta alle tecniche crittografiche utilizzate.

A loro volta, gli *smart contract* consistono in protocolli per computer, basati sulla logica "*if this, then that*", che elaborano in modo autonomo le istruzioni programmate una volta soddisfatte le regole di condizionalità e che possono beneficiare delle caratteristiche della *blockchain* alla quale sono "agganciati". Attraverso la "catena di blocchi" è possibile, inoltre, gestire l'emissione e la circolazione di una valuta digitale, accettata e scambiata da tutti i partecipanti.

Nella prassi, esistono tipologie diverse di *blockchain*.

Le tecnologie *blockchain* si distinguono, infatti, a seconda delle modalità di accesso alla rete (*unpermissioned*/*permissioned*) e di accesso ai dati (*pubblico/privato*).

Nelle *blockchains unpermissioned* o "non autorizzate", non sono previste riserve per partecipare alla rete, a qualsiasi titolo; nelle "*permissioned*", invece, la costruzione del consenso e convalida delle transazioni sono riservate a certi nodi.

Nelle pubbliche i dati sono accessibili pubblicamente; nelle private, invece, l'accesso ai dati è limitato [38].

Nel nostro ordinamento, l'art. 8-*ter*, comma 3, del d.l. 14 dicembre 2018, n. 135 (c.d. Decreto Semplificazioni), convertito nella legge 11 febbraio 2019, n. 12, fornisce la definizione di "Tecnologie basate su registri distribuiti e *smart contract*" (con la precisazione che, per quanto fin qui evidenziato, le *Distributed Ledgers Technology* o DLT sono un *genus* che include la *blockchain*, ma non si esaurisce in essa). Le prime sono "le tecnologie e i protocolli informatici che usano un registro condiviso, distribuito, replicabile, accessibile simultaneamente, architetturalmente decentralizzato su basi crittografiche, tali da consentire la registrazione, la convalida, l'aggiornamento e l'archiviazione di dati sia in chiaro che ulteriormente protetti da crittografia, verificabili da ciascun partecipante, non alterabili e non modificabili" (comma 1); per "*smart contract*" si intende, invece, "un programma per elaboratore che opera su tecnologie basate su registri distribuiti e la cui esecuzione vincola automaticamente due o più parti sulla base di effetti predefiniti dalle stesse. Gli *smart contracts* soddisfano il requisito della forma scritta previa identificazione informatica delle parti interessate, attraverso un processo avente i requisiti fissati dall'Agenzia per l'Italia Digitale con linee guida da adottare entro novanta giorni dalla data di entrata in vigore della legge di conversione del presente decreto" (comma 2).

Al riguardo, le Linee Guida dell'AGID, adottate il 7 maggio 2020, per la modellazione delle minacce e individuazione delle azioni di mitigazione conforme ai principi del *secure/privacy by design* [39] specificano che le DLT "sono sistemi informatici che gestiscono dati, transazioni o codici eseguibili (*Smart Contracts*) in modo il più possibile indipendente da un'autorità centrale attraverso l'utilizzo di *data storage* distribuito in correlazione con processi crittografici e sistemi decisionali decentralizzati".

Le linee guida appena citate risultano di particolare interesse, perché forniscono indicazioni agli sviluppatori per la progettazione di "catene di blocchi" sicure e in grado di prevenire rischi per la tutela dei dati personali.

Come specificato nelle Linee Guida, il loro ambito è esteso a tutte le applicazioni della tecnologia *blockchain*, come ad esempio:

"sistemi di identità digitale (*Self Sovereign Identity*);

sistemi di certificazione garantita di dati e certificazioni (*Verifiable Claims*);

creazione e gestione di nuovi mercati digitali (vedi i mercati *peer to peer* di scambio energetico) fino alla creazione e gestione di nuove entità (vedi ad esempio le DAO/DAC *Distributed Autonomous Organizations/Corporations*)".

Con riferimento all'integrità dei dati, le Linee Guida hanno evidenziato che "uno dei fattori fondamentali che assicurano tale caratteristica in una DLT è la struttura a blocchi concatenati attraverso la funzione di *hash*" (o "*message digest*"/"*digest*", ossia soluzioni crittografiche che forniscono la stringa a lunghezza fissa di un messaggio), per cui "la modifica di un blocco in posizione <n> implicherebbe la conseguente modifica di tutti i blocchi successivi fino alla testa della catena". Ad ogni modo, tale caratteristica "di per sé non basterebbe se non fosse affiancata da un adeguato algoritmo di consenso che garantisca l'immediata evidenza di una qualsivoglia modifica di questa struttura in confronto a strutture uguali esistenti nei vari nodi componenti la DLT".

Con riguardo alla disponibilità dei dati, le Linee Guida hanno affermato che "è intrinsecamente garantita dall'infrastruttura sottostante: difatti ogni nodo di una DLT (a meno di nodi specifici, normalmente chiamati "*light nodes*") detiene una intera copia della struttura dati e quindi l'indisponibilità degli stessi si potrebbe avere solo nel caso in cui tutti i nodi fossero allo stesso istante inattivi".

Di conseguenza, un attacco alla disponibilità dei dati è reso più difficoltoso, perché dovrebbe avere come obiettivo non la struttura decentralizzata, ma l'intera infrastruttura (ad es., il *software* di base).

Per quanto attiene la riservatezza dei dati, l'AGID ha sottolineato che essa varia a seconda delle caratteristiche della tecnologia utilizzata. Secondo le Linee Guida, "alcune DLT sono intrinsecamente trasparenti (vedi *bitcoin*) in quanto chiunque ha accesso a tutte le transazioni fatte da qualsivoglia partecipante e la confidenzialità è demandata all'anonimità dei partecipanti che vengono identificati da un indirizzo generico". In realtà, sembrerebbe più corretto fare riferimento alla nozione di pseudoanonimizzazione, per come già chiarita *supra*, laddove sia comunque possibile risalire all'identità della persona interessata alla quale il dato si riferisce.

Ad ogni modo, le Linee Guida raccomandano agli sviluppatori di provvedere, "in qualsiasi caso", a una "adeguata gestione della riservatezza dei dati in modo disgiunto dalla gestione dell'infrastruttura: il livello di riservatezza da implementare sarà come al solito legato alla tipologia dei dati e le metodologie le stesse applicate a qualsiasi altra tipologia di *data storage*".

L'AGiD ha individuato, inoltre, gli attacchi più frequenti ai quali sono esposte le tecnologie DLT, per lo più diretti verso le applicazioni (*smart contracts*) che girano di esse, anziché sulla *chain* stessa. Di conseguenza, l'Autorità ha suggerito agli operatori di prestare attenzione alla "qualità delle applicazioni che operano sulla DLT e prevedere per le stesse lo stesso ciclo di controllo di un qualsiasi *software* sviluppato come da linee guida AGID".

Le Linee Guida dell'AGID costituiscono un punto di riferimento rilevante ai fini dello sviluppo di una piattaforma basata su *blockchain*, ma non esauriscono tutte le questioni che tale nuova gamma di tecnologie pone in riferimento al trattamento dei dati personali.

Come già sottolineato, le *blockchains* rendono ardua l'individuazione del ruolo di titolare e di responsabile del trattamento e, di conseguenza, anche la chiara identificazione e ripartizione delle eventuali responsabilità.

La questione risulta di particolare complessità specie nelle *blockchain* pubbliche e *permissionless*, che operano con la sostituzione del tradizionale modello *client-provider* con uno basato sull'elaborazione collettiva dei dati attraverso un protocollo condiviso [40]. Secondo una prima interpretazione i *miners* (ossia, come già evidenziato, i validatori della transazione, tramite creazione di blocchi) sono *data processors* e il *data controller* è chi ha in carico la *blockchain*. Secondo un'altra tesi, ogni nodo nella rete *peer to peer*

contenente dati personali dovrebbe essere trattato separatamente, e se il *miner* determina perché e come la sua versione locale del blocco viene elaborata, allora è un data controller. Di conseguenza, ogni *miner* è un titolare e ha la piena responsabilità del trattamento del suo blocco. Secondo un'ulteriore lettura, la *blockchain* sarebbe un'entità unica, ma ogni *miner* è un *data controller* insieme a tutti gli altri, con cui determina perché e come i dati vengono elaborati [41].

La difficoltà nell'individuazione del *data controller* e i correlati ostacoli nell'attuazione concreta dell'impianto del GDPR, basato su una centralizzazione del rischio in capo al titolare del trattamento, sono state evidenziate anche dal Parlamento dell'Unione Europea, nello studio "*Blockchain and the General Data Protection Regulation*", del 24 luglio 2019.

Nel documento intitolato *"Blockchain and the GDPR: Solutions for a responsible use of the blockchain in the context of personal data"*, del 28 novembre 2018, la *Commission Nationale Informatique & Libertés* (CNIL), ossia l'Autorità garante francese, ha tentato di fornire alcune indicazioni al riguardo.

Secondo il CNIL, infatti, in molti casi, il partecipante (ossia chi decide di registrare i dati su una *blockchain*) può essere considerato titolare del trattamento, "*given that the participant determines the purpose and means of data processing*".

Nel documento intitolato "*Solutions for a responsible use of the blockchain in the context of personal data*", la stessa Autorità ha affermato che i *"participants, who have the right to write on the chain and who decide to send data for validation by the miners, can be considered as data controllers.*

Indeed, blockchain participants define the purposes (objectives pursued by the processing) and the means (data format, use of blockchain technology, etc.) of the processing".

Nel dettaglio, il CNIL ha sostenuto che il *partecipant* è un *data controller*:

• "*when the said participant is a natural person and that the personal data processing operation is related to a professional or commercial activity (i.e. when the activity is not strictly personal);*

• *when the said participant is a legal person and that it registers personal data in a blockchain*".

Il criterio discretivo per l'individuazione del *data controller* resta, dunque, quello incentrato sulla possibilità di decidere come e perché trattare i dati.

Secondo il CNIL, inoltre, nell'ambito delle "catene di blocchi", possono essere considerati responsabili, ai sensi del GDPR:

• gli *smart contract developers*, che hanno il compito di processare i dati per conto del titolare;

• in alcuni casi, i *miners* che seguono le istruzioni dei *data controllers*, quando controllano se la transazione soddisfi i criteri tecnici.

Ad ogni modo, costoro dovrebbero stipulare un contratto con il *data controller*, che specifichi gli obblighi di ciascuna parte e che riproduca le disposizioni dell'art. 28 del GDPR.

Lo stesso CNIL ha soggiunto, però, di essere consapevole delle difficoltà che la qualifica di *miners* come *data processors* potrebbe generare e ha esortato gli *stakeholders* a elaborare soluzioni innovative sul tema.

Di particolare interesse, risulta la raccomandazione dell'Autorità francese, secondo cui "*When a group of entities decides to carry out processing operations on a blockchain for a common purpose: • the CNIL recommends that the participants take a common decision about the data controller's responsibilities: ▪ either*

by creating a legal person to be the data controller; ▪ or by designating the participant that makes decisions for the group as the data controller; • otherwise, all participants are likely to be considered as being joint controllers".

Con riguardo agli sviluppatori del protocollo, nel report dedicato al GDPR, l'EU Blockchain Observatory and Forum suggerisce che non siano considerati *data controllers*, perché costoro lavorano volontariamente a un software che non li remunera in modo diretto, non decidono circa l'adozione degli aggiornamenti della piattaforma (che si limitano a suggerire) e, di regola, non influiscono sulle finalità di quest'ultima.

Con riferimento agli utenti della rete che firmano e inviano transazioni alla rete *blockchain* attraverso un nodo, l'EU Blockchain Observatory and Forum ha evidenziato che *"If they submit personal data to the blockchain ledger as part of a business activity, they are most likely to be considered data controllers. this would include entities that operate software as well as products or services that post personal data onto a blockchain (which is not recommended). however, if they submit their own personal data for their own personal use, for example to buy or sell crypto-assets, they are likely to fall under the household exemption of the GDPR and may not be considered data controllers".*

Con riguardo agli smart contracts *"there is a debate as to whether this software should be seen as being operated by its publisher, by the network user calling it or by both. This debate will probably have to be resolved on a case-by-case basis".*

Sussistono poi dei contrasti sulla riconducibilità di *hash*/chiavi pubbliche in *blockchain*, riferiti a dati di persone fisiche, alla nozione di dati personali prevista dal GDPR (su cui si rinvia *supra*).

Con la "catena di blocchi", le transazioni eseguite non rivelano direttamente l'identità delle parti, ma sono collegate a una chiave pubblica/*hash*. Secondo la tesi minoritaria non si tratterebbe di dati personali, perché le soluzioni crittografiche non servirebbero a celare identità, ma a risolvere un problema tecnico. Al riguardo, è stato sottolineato che l'equazione chiave pubblica-dato (personale) pseudonimizzato è errata perché *"it's worth pointing out that a public key is used in a blockchain without openly stating who is the holder of the corresponding private key (unless the relevant holder decides to). Furthermore, a public key is not always associated with a natural person's address".* Ad ogni modo, secondo tale tesi, anche quando la coppia di chiavi è usata da una persona fisica, tale equivalenza mostra i suoi limiti e si rivela errata, perché la soluzione crittografica non è utilizzata per l'identificazione del mittente e della paternità del documento, come accade in caso di posta elettronica certificata e di software di firma digitale. *"On the contrary, in a blockchain, everybody may perform a transaction without assigning anidentity in the network to the creditor or the debtor, and it is not possible to track down theidentity of the parties to a transaction without using advanced means of digital forensic and bigdata analysis, making questionable assumptions (e.g. correspondence between IP address anduser), having access to confidential information which may be disclosed only with an orderissued by the Authority"* [42]. Secondo la tesi prevalente, invece, *hash*/chiavi pubbliche, se incrociate con altre informazioni, potrebbero consentire di risalire agli autori della transazione e costituire, dunque, dati personali, come tali sottoposti alle garanzie previste dal GDPR [43]. A proposito della possibilità di considerare personali i dati di una persona fisica criptati o sottoposti ad *hash*, nello studio "*Blockchain and the General Data Protection Regulation Can distributed ledgers be squared with European data protection law?*", del giugno 2019, l'European Parliamentary Research Service (EPRS), "*Whereas it is often assumed that this is not the case, such data likely does qualify as personal data for GDPR purposes, meaning that European data protection law applies where such data is processed*".

Al riguardo, l'EPRS ha richiamato l'*Article 29 Working Party*, *Opinion* 05/2014 *on Anonymisation Techniques* (WP 216) 0829/14/EN, 20, nella parte in cui ha avvertito che le funzioni di *hash* possono ridurre la riconducibilità di un set di dati con l'identità originale di un soggetto e, dunque, costituiscono una misura di sicurezza utile, ma non un metodo di anonimizzazione (su cui si rinvia *supra*).

L'EPRS ha sottolineato, tuttavia, che esistono delle funzioni di *hash* con garanzie di privacy particolarmente forti, che – secondo una valutazione caso per caso – potrebbero essere in grado di resistere al test dei "mezzi ragionevolmente probabile che vengano utilizzati", di cui al considerando 26 del GDPR.

Al riguardo, pare opportuno ricordare che nel *whitepaper* "*Development of a GDPR-compliant blockchain solution for the german asylum procedure*", redatto, nel 2019, dal *Federal Office for Migration and Refugees*, come guida nella creazione di una *blockchain* conforme al GDPR per la procedura d'asilo in Germania, è evidenziato che la memorizzazione di dati personali sulla catena di blocchi è da evitare. I dati personali dovrebbero rimanere nei sistemi di *back-end*. Secondo la valutazione dell'Ufficio federale, inoltre, ciò dovrebbe applicarsi anche a tutti i valori *hash* che si riferiscono a dati personali, poiché i progressi nella potenza di calcolo potrebbero renderli reversibili con uno sforzo gestibile.

L'Autorità ha soggiunto che "*Of further critical signifcance are specifc references on the blockchain. As soon as data stored on the blockchain can be used to identify an individual person, it constitutes personal data and is thus subject to the GDPR. Accordingly, the data on the blockchain should be kept to a minimum, and existing IDs should not be used in the blockchain".*

A tale proposito, nel documento sopra menzionato, il CNIL ha specificato che la catena di blocchi può contenere due tipi di dati personali, ossia:

"participants' and miners' identifiers: each participant/miner has a public key, ensuring identification of the issuer and receiver of a transaction;

additional data contained "within" a transaction (e.g.: diploma, property deed). If such data concerns natural persons, possibly other than the participants, who may be directly or indirectly identified, such data is considered personal data".

Per l'Ufficio federale tedesco, laddove la *blockchain* presenti necessariamente dati personali, occorre che la progettazione avvenga in modo tale che una persona non possa essere identificata senza ulteriori informazioni. A questo fine, deve essere adottata una tecnica di pseudonimizzazione.

La *blockchain* potrebbe rendere, inoltre, difficile l'esercizio di alcuni diritti previsti dal GDPR a tutela dell'interessato (su cui si rinvia *supra*).

Come già evidenziato, tra i diversi diritti del *data subject*, vi è quello alla cancellazione dei dati personali. Tale diritto mal si concilia, tuttavia, con la *blockchain,* basata sulla conservazione dei dati su cui "si struttura", al punto che la rottura della catena di blocchi scardina la sicurezza del sistema.

Secondo il CNIL è tecnicamente impossibile accogliere la richiesta di cancellazione dei dati dell'interessato registrati su una *blockchain*. "*However, when the data recorded on the blockchain is a commitment, a hash generated by a keyed- hash function or a ciphertext obtained through "state of the art" algorithms and keys, the data controller can make the data practically inaccessible, and therefore move closer to the effects of data erasure*".

Ai nostri fini, occorre evidenziare che il diritto alla cancellazione non opera, ai sensi di quanto previsto dall'art. 17, par. 3 GDPR, dato che non può essere riconosciuto all'interessato quando il trattamento dei dati personali è necessario d) per motivi di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici.

Nel bilanciamento di interessi, infatti, per espressa scelta normativa, risulta prevalente quello alla ricerca.

Al riguardo, la dottrina [44] ha sottolineato che analoga previsione non sussiste con riferimento ad altri diritti, come quello di rettifica (su cui si v. *supra*).

A tale proposito, occorre evidenziare che anche l'attuazione del diritto alla rettifica nel sistema *blockchain* risulta non agevole, ma "meno complessa del diritto di cancellazione *tout court*, dal momento che in presenza di un consenso (*consensus*) tra i partecipanti non è tecnicamente impossibile fare "deviare" una catena dal suo corso, interrompendola in corrispondenza al dato da rettificare e facendole assumere una nuova direzione. Questa opzione è definita tecnicamente "*forking"* e consiste nel modificare sia il dato rettificato sia tutti i dati successivi che da questo "a cascata" discendono" [45].

Secondo l'Ufficio federale tedesco, per mezzo di soluzioni di mappatura *off-chain* (in grado di collegare le caratteristiche di riferimento pseudonime sulla *blockchain* con quelle specifiche utilizzate dalle rispettive autorità), è possibile rispettare il diritto di rettifica e di cancellazione, "*by 'rectifying' the data through rectifcation transactions, and by deleting the mapping, they can depersonalise the data on the blockchain from their subjective perspective, i.e. 'delete' it*".

Al riguardo, il CNIL ha affermato che il diritto di rettifica potrebbe essere realizzato con l'inserimento dei dati aggiornati in un nuovo blocco. "*Indeed, a subsequent transaction can cancel an initial transaction, even though the first transaction will still appear in the chain. The same solutions as those applied following a request for deletion of personal data could be applied to erroneous data when such data requires deletion*".

Il Comitato economico e sociale europeo, in occasione del parere sul tema «Blockchain e mercato unico dell'UE: le prossime tappe», pubblicato l'11 febbraio 2020 [46], ha esortato la Commissione europea "a esaminare il regolamento e a proporre revisioni e fornire ulteriori indicazioni sul rapporto tra il GDPR e la blockchain". Nel frattempo, proprio con riferimento all'impiego della nuova tecnologia nel settore energetico, alcuni studiosi suggeriscono di "utilizzare specifiche funzionalità delle piattaforme *blockchain*; ad esempio, in *Hyperledger Fabric*, l'uso dei 'dati privati' e dei canali consente di definire in modo puntuale l'ambito di visibilità delle informazioni scritte sulla *blockchain*. I canali costituiscono infatti delle *blockchain* parallele, e i 'dati privati' restringono ulteriormente l'accesso ad un sottoinsieme di organizzazioni presenti sul canale" [47].

2.9 Casi di studio

L'esame dei profili rilevanti ai fini del trattamento dei dati personali deve essere condotto distintamente per ciascuno dei moduli applicativi in cui si articola/potrebbe articolarsi il progetto di ricerca:

A. **adesione di utenti residenziali alla sperimentazione di una rete di *Smart Home***, tramite l'istallazione a titolo gratuito di una serie di **sensori** per il monitoraggio dei consumi elettrici, del confort e presenza all'interno della propria abitazione connessi ad una piattaforma (https://dhomus.smartenergycommunity.enea.it/)

B. **piattaforma web (https://www.smarthome.enea.it/smartsim/login)** su cui un qualsiasi utente compilando una **scheda-questionario**, ovvero inserendo dei dati relativi alla propria abitazione, utenze e consumi relativi alla propria abitazione, utenze e consumi potrà avere una serie di ***feedback*** per incrementare la propria consapevolezza energetica e indicazioni per risparmio energetico ed economico connesso ad alcuni suggerimenti customizzati in base alle informazioni fornite dall'utente stesso.

C. **piattaforma *Local Energy Community*** (di seguito LEC) per *local token economy*, basata su *blockchain* e finalizzata allo scambio di beni e servizi con *token*, tramite *smart contract*.

D. **fusione dei casi A e C**, con la peculiarità che l'utente è (necessariamente) anche membro di una **comunità energetica** (facente parte di una LEC più ampia).

E. **piattaforma in grado di monitorare i *social media web*** per estrarre alcune conoscenze afferenti le comunità energetiche senza alcuna supervisione umana.

2.10 Caso A - Dimostrativo sperimentale con acquisizione dati in tempo reale

Il primo caso prevede la sperimentazione di un prototipo di "*smart home"* su un numero ristretto di abitazioni in cui è previsto il monitoraggio in tempo reale di una serie di parametri, tramite l'istallazione di sensori in grado di acquisire i dati e inviarli a una piattaforma *cloud*.

La *"smart home*" ideata da ENEA consente, infatti, di monitorare e di ottimizzare i consumi energetici, oltre al livello di comfort e di sicurezza di abitazioni e degli uffici di un distretto residenziale e terziario, per poi inviare i dati acquisiti a un'apposita **piattaforma**. L'unità centrale, ossia la piattaforma, è il luogo in cui i dati trasmessi sono analizzati ed aggregati al fine di fornire un serie di *feedback* all'utente e alla comunità, per ridurre i consumi di energia elettrica e termica, anche attraverso un confronto virtuoso, ancorché anonimo, con i livelli di dispendio energetico dei vari partecipanti alla sperimentazione.

Nelle specie, tramite portale o applicazione *smartphone*, il POD consente il monitoraggio dei consumi rilevati dal contatore e quello della generazione di energia elettrica prodotta da fonti rinnovabili installate nelle abitazioni degli aderenti alla sperimentazione, il controllo dell'energia e dello stato del sistema di accumulo, la certificazione delle movimentazioni di energia effettuate per erogare la flessibilità (tra utenti finali, società di vendita e aggregatori), il monitoraggio dei "premi" e delle "penalità" conseguite.
Tramite accesso ad apposita piattaforma, ENEA consente, invece, il monitoraggio dei dati acquisiti dalla sensoristica installata e la fruizione dei servizi messi a disposizione degli aderenti alla sperimentazione, ossia: la certificazione della propria flessibilità elettrica tramite tecnologia *blockchain*, *feedback* customizzati sui propri consumi, i confronti con utenti simili (per composizione di nucleo familiare e tipologia di utenza). Al contempo, gli utenti sperimentatori dei sistemi di *smart home* testati nel progetto avranno la possibilità di interagire con gli strumenti appena descritti per rispondere alla richieste di flessibilità provenienti dalla rete.

La **finalità del trattamento** è quella di ricerca scientifica.

Durante la fase di sperimentazione i dati potranno essere forniti in forma anonima ai *partner*s del progetto di ricerca per analisi e sviluppo di algoritmi di previsione, disaggregazione, ecc.

Gli interessati sono gli utenti che hanno aderito spontaneamente alla sperimentazione.

L'acquisizione del **consenso** è avvenuta tramite apposita **informativa**, con invio del modulo **in fase di richiesta di adesione** per sola presa visione (dunque prima del *download*/installazione o della registrazione alla piattaforma).

I **contitolari** del trattamento dati sono ENEA, per la sua piattaforma, e il gestore/i gestori della rete di distribuzione coinvolti.
L'adesione è funzionale a rendere dei **servizi all'utente**.

Le categorie di dati personali trattati dall'ENEA sono:

a) **dati anagrafici, dati di contatto e indirizzo** di abitazione dei partecipanti alla sperimentazione, conferiti dagli stessi in sede di adesione volontaria;
b) dati relativi ai consumi elettrici degli elettrodomestici, alla presenza degli occupanti e ai parametri ambientali, raccolti tramite i sistemi di gestione energetica installati dall'ENEA presso le abitazioni dei partecipanti; dati relativi ai consumi elettrici monitorati dai contatori elettrici di seconda generazione installati dal DSO, i dati relativi alla eventuale produzione e immagazzinamento dell'energia elettrica

tramite fotovoltaico e *storage* installato e i dati necessari alla corretta valutazione della soluzione da implementare.

I dati *sub* a) saranno archiviati, per un tempo predeterminato, in un *database* accessibile unicamente al personale autorizzato al trattamento che operano sotto l'autorità dell'ENEA.
I dati *sub* b) saranno archiviati, per un tempo predeterminato, in un *database* separato, accessibile sia al personale autorizzato allo svolgimento dei trattamenti correlati alle attività progettuali, sia allo sviluppatore del *software* e titolare del sistema operativo. I dati raccolti attraverso i sensori saranno corredati da un codice univoco ("codice abitazione") attribuito alle singole unità abitative, per impedirne la riconducibilità immediata ai soggetti interessati, che resterà prerogativa del personale autorizzato dell'ENEA.

Il *server* e i singoli *database* sono protetti con un sistema di autenticazione conforme alle *best practices* correnti per la minimizzazione dei rischi di accesso non autorizzato. Al contempo, la comunicazione tra la piattaforma collegata al sistema di sensoristica e il *database* di destinazione dei dati oggetto di monitoraggio è protetta e criptata, a salvaguardia dell'autenticità della provenienza e dell'integrità dei dati.
In tal modo, si tenta di agevolare l'attuazione del principio di minimizzazione anche sotto il profilo organizzativo, rafforzando l'efficacia delle misure di pseudonimizzazione descritte in precedenza: la possibilità di ricongiungere i "codici abitazione" ai partecipanti alla sperimentazione richiederà, infatti, specifici livelli di autorizzazione all'accesso, riducendo i rischi di re-identificazione degli interessati.

L'interessato può accedere in tempo reale ai dati monitorati e ai dati storici relativi esclusivamente al proprio sistema. Il confronto con gli utenti simili per composizione di nucleo familiare e tipologia di utenza non consente di identificare gli altri partecipanti al confronto.

Gli utenti possono esercitare il diritto all'oblio, che prevede la totale rimozione dei dati preservati in qualsiasi momento avvenga la richiesta.

I soggetti, terzi rispetto all'ENEA e al personale autorizzato che opera sotto l'autorità della stessa, che potranno avere conoscenza dei dati raccolti nell'ambito delle attività progettuali, sono:
i) la società che eseguirà le attività di installazione e manutenzione dei sensori per conto dell'ENEA. A tal fine tratterà, in qualità di Responsabile del trattamento, i dati indicati sub a). I rapporti con il Titolare e le specifiche istruzioni di trattamento saranno formalizzate in conformità dell'art. 28 del GDPR.
La società, inoltre, avrà accesso diretto e in tempo reale, con credenziali *Administrator*, al *database* contenente i dati sub b) del paragrafo precedente (con la precisazione, che, come anticipato, tuttavia, la riconducibilità dei dati ai soggetti interessati sarà consentita al solo personale autorizzato dell'ENEA, tramite le misure di pseudonimizzazione sopra indicate);

ii) DSO avente "dominio" dello *smart meter*, con cui è stipulato un accordo di collaborazione su tematiche inerenti lo sviluppo di *energy communities*. Il DSO promuoverà l'istallazione di contatori di nuova generazione nelle abitazioni oggetto della sperimentazione, che potranno comunicare direttamente con i sistemi di gestione predisposti da ENEA, fornendo direttamente i dati sul consumo generale dall'appartamento, la produzione da fotovoltaico e lo stato dell'eventuale batteria presente nelle abitazioni. Il ruolo attribuibile al DSO, rispetto al trattamento dei dati personali dei partecipanti al progetto, potrà essere definito in maniera puntale all'esito di una ulteriore attività di analisi documentale (tenendo conto, in particolare, dell'accordo di collaborazione in essere) e raccolta di informazioni.

Nel caso in cui nel corso della sperimentazione dovessero aggiungersi ulteriori utenze, afferenti ad altri progetti, il documento base dovrà essere aggiornato per consentire l'inclusione di eventuali ulteriori soggetti.
L'eventuale diffusione dei dati avverrà solo in forma aggregata o completamente anonima per report di progetto o per pubblicazioni scientifiche.
I dati personali raccolti potranno essere trasferiti all'estero.

2.11 Caso B – Utenti piattaforma che compilano un questionario

Il secondo caso prevede, invece, la compilazione di un questionario on-line da parte di un utente residenziale. I dati richiesti sono i seguenti:

a) dati sull'utente (non include dati anagrafici);
b) dati sulle caratteristiche architettoniche della sua abitazione;
c) dati sui suoi impianti;
d) dati sui suoi elettrodomestici;
e) dati sui suoi consumi elettrici.

I dati acquisiti sono inseriti da un'applicazione *software* in un modulo di calcolo, che fornisce una serie di ***feedback* di *output***, secondo quanto segue:

1. Ripartizione consumi di energia primaria per servizio (riscaldamento, raffrescamento, acqua calda sanitaria, cucina, refrigerazione, lavaggio, pulizia e stiratura, illuminazione, computer e internet, cura della persona, altro)
2. Tipologia dei carichi elettrici (accumulabili, differibili, non differibili)
3. Elettrificazione dell'abitazione
4. Confronti con benchmark di riferimento
5. Possibili migliori tariffe di fornitura elettricità e gas
6. Potenziale di elettrificazione dell'abitazione
7. Potenziale di risparmio energetico dell'abitazione

Può accedere al servizio chiunque si registra al sito, fornendo un indirizzo e-mail valido, al quale vengono inviate le credenziali di accesso alla piattaforma (codice identificativo univoco e password).

L'indirizzo e-mail richiesto per le credenziali di accesso è conservato al fine di:

- consentire il recupero delle credenziali in caso di smarrimento;
- gestire l'autenticazione dell'utente in caso di accessi successivi alla piattaforma per consultare ed eseguire il *download* dei *feedback* di *output*, completare la compilazione del questionario o modificare i dati precedentemente inseriti;
- inviare copia dei *feedback* di *output* alla casella di posta elettronica dell'utente, in forma di allegato.

In ogni caso, l'associazione tra l'indirizzo e-mail e le credenziali di accesso, così come tra i dati acquisiti tramite la compilazione del questionario e l'indirizzo e-mail e/o codice identificativo assegnato all'utente, è consentita solo al personale autorizzato dell'ENEA.

Se l'utente è già registrato alla piattaforma ed è, dunque, già in possesso di un codice identificativo, può inserirlo direttamente nell'apposito *form* (previo processo di controllo sull'effettiva presenza del codice inserito nel *database*).
Se l'utente non è in possesso del codice identificativo, si dovrebbe prevedere una procedura per la generazione automatica di un codice valido e alfanumerico, che non sia già presente nel database.

I dati sono conservati su un *database on premises* nell'intranet ENEA, non accessibile dall'esterno.

L'accesso al *database* è consentito, per un tempo predeterminato, a:
- soggetti autorizzati che operano sotto l'autorità di ENEA (titolare del trattamento), incluso il personale preposto allo sviluppo software;

- sviluppatori esterni, solo per le operazioni di gestione operativa e manutenzione della piattaforma;
- analizzatori dei dati per adeguamento dinamico dei *benchmarking*, validazione ecc., che operano presso Università che collaborano con il progetto.

2.12 Caso C – Utenti della sperimentazione Local token Economy

Il caso riguarda il modello ENEA di *Local Token Economy*, sviluppato internamente al Progetto Ricerca di Sistema Elettrico. Il prototipo tiene conto dell'impatto potenziale della digitalizzazione e dei modelli di economia collaborativa sul processo di transizione energetica e prende spunto dall'analisi congiunta di casi di studio di comunità energetiche e di esperienze di valute comunitarie digitali a livello internazionale. In particolare, si prospetta un modello di *microgrid* virtuale *peer to peer*, basata sull'impiego della tecnologia *blockchain*, che dovrà abilitare la reciprocità degli scambi tra *prosumer*s e consumatori locali, in ambito sociale oltreché energetico.
L'idea di base è quella di fare riferimento al quadro normativo della *Renewable Energy Community*, il che significa:

- focalizzarsi sul vettore elettrico;
- ammettere la partecipazione di cittadini, piccole imprese ed autorità locali al progetto;
- avere come finalità principale il raggiungimento della sostenibilità sociale, economica e ambientale.

La comunità è caratterizzata dalla compresenza di obiettivi e di comportamenti differenti da parte dei diversi attori, come in qualsiasi contesto economico e sociale che possa autosostenersi. Per questo motivo, la piattaforma che supporta i Servizi di *Local token Economy*, attraverso la tecnologia *blockchain*, deve gestire l'emissione e la circolazione di una *Community Inclusive Currency* (CIC), ossia una valuta comunitaria digitale, che venga accettata e scambiata da tutti i partecipanti della comunità.
La CIC avrà la funzione di premiare la messa in comune, da parte dei singoli partecipanti, di competenze e di tempo per erogare servizi di assistenza sanitaria, baby-sitting, *co-learning* e servizi di natura ecologica.
Allo stato attuale, il caso posto riguarda **un servizio relativo ad una lezione di danza tra un cittadino docente di danza moderna (erogatore), cittadino interessato al corso (fruitore), pubblica amministrazione proprietario di un salone (*stakeholder*).**
Il **trattamento dati** riguarda:
Dati di registrazione alla piattaforma LEC su cui viene proposto il servizio, dove l'anagrafica di registrazione include nome, cognome, indirizzo, città, provincia, e-mail e codice fiscale (sia per cittadino sia per lo *stakeholder*).
Dati di offerta del servizio: comprende il portafoglio *token* e il dato di georeferenziazione per il luogo di erogazione del servizio. Dati inerenti la struttura messa a disposizione (ubicazione, grandezza, capienza) e relativo costo in *token*. Dati relativi alla avvenuta fruizione del servizio (dati di fruizione servizio, annotazioni di *token* trasferiti su *blockchain*).
I dati vengono acquisisti in specifici *forms* sviluppati in piattaforma LEC. Vi saranno *form* differenti per:
Dati registrazione (*form* di registrazione *on-line*, dove l'adesione è funzionale a rendere dei **servizi all'utente)**.
Dati del servizio (*form* di offerta di servizio);
Dati fruizione del servizio (*form* di accettazione e conferma del servizio).
Sulla base delle informazioni sussistenti allo stato attuale dello sviluppo della piattaforma è emerso che il **titolare** del trattamento dati è ENEA.
Occorrerà poi definire il ruolo dei nodi validatori, anche alla luce delle caratteristiche della *blockchain* (al momento ancora *in progress*).
Il trattamento dei dati coinvolge, inoltre, ulteriori soggetti, ossia: l'amministratore della piattaforma web, l'amministratore della comunità, i ricercatori impegnati su algoritmi, il gestore *token economy* (include *blockchain*).
Rispetto ai dati sopra elencati occorre precisare che quelli anagrafici vengono gestiti da ENEA, dall'amministratore piattaforma *web* e dall'amministratore della comunità; i dati del servizio e del portafoglio *token*, invece, da ENEA, dall'amministratore piattaforma *web*, dall'amministratore della comunità e dal gestore *token economy* (inclusa la *blockchain*).

Occorre evidenziare, infine, che l'archivio dati si trova in un *database on-premises*, interno alla rete ENEA.
Per esigenze di funzionalità il *database* è accessibile dall'esterno attraverso accessi controllati e ristretti al minimo necessario per la funzionalità del servizio (via WEB e via APP).
La struttura del *database* è compartimentata con logiche di sicurezza, in modo da impedire accessi non strettamente funzionali agli obiettivi del servizio.
I dati personali anagrafici sono oggetto di *storage* dedicato separato. I dati sono pseudoanonimizzati (su due differenti *databases* con chiave di relazione) in modo da impedirne la riconducibilità diretta al soggetto. Il dato gestito in *blockchain* è, infatti, su un *database* differente rispetto ai dati di anagrafica, per evitare l'immediata riconducibilità all'interessato; esiste poi un codice che mette in relazione le due tabelle e le relative informazioni.
La conservazione dei dati anagrafici avverrà per la durata del progetto (2021) e per 12 mesi dopo la fine del suo *follow-up* (2022-24) ai fini di ricerca.
Eventuali installazioni del *software* presso gestori di LEC avverranno azzerando i dati e con regole di gestione esplicitamente definite dal gestore.
Con riguardo al trattamento appena menzionato e brevemente descritto, occorre evidenziare che, l'esatta perimetrazione dei ruoli spettanti a coinvolti nel trattamento dati (ad oggi, *in progress*) sarà, tuttavia, di estremo rilievo per consentire al DPO di ENEA di individuare i titolari, i responsabili/incaricati nell'ambito del trattamento (e di definire accordi per delimitare le rispettive responsabilità). Occorre segnalare, inoltre, la necessità di stipulare un contratto con la società proprietaria della strumentazione per il rilievo/acquisizione dati, di cui si avvale il *partner* di progetto, al fine di chiarire i compiti di tale soggetto nell'ambito del trattamento dati.
Del pari, occorre definire puntualmente le caratteristiche della *blockchain* da utilizzare.
Sulla base di quanto sopra evidenziato, con riferimento ai rapporti tra la "catena di blocchi" e il GDPR, l'uso di una *blockchain* privata e locale sembrerebbe la soluzione più congeniale ai fini della migliore gestione del trattamento dati degli utenti.
Ad ogni modo, si rinvia alle considerazioni sviluppate nella parte generale, come ausilio per la ricostruzione e la risoluzione delle principali problematiche in tema di *privacy* connesse alla realizzazione della *Local token economy*.
Si segnala, inoltre, che la struttura del *database* dovrà essere elaborata in conformità del GDPR.
Del pari, occorre considerare che gli *smart contracts*, in esecuzione di una *blockchain*, che comportano l'uso di dati personali, sono il portato di decisioni automatizzate e, dunque, il GDPR deve essere preso in considerazione durante la loro configurazione.

2.13 Caso D – Adesione alla comunità energetica

Il caso concerne il cittadino (avente una o più utenze, in caso in edifici differenti in un area territoriale estesa) che intende aderire a una comunità energetica. Tale partecipazione comporta una liberatoria per l'accesso ai dati del contatore da parte dell'utente-aderente.
La fattispecie in oggetto fonde i due casi A e C, con la peculiarità che nell'ipotesi in esame l'utente è (necessariamente) anche membro di una comunità energetica (che è parte di una LEC più ampia).
Gli interessati sono, dunque, gli utenti, partecipanti alla *energy community*.
Il caso riguarda, quindi, il progetto di realizzazione di una comunità energetica, con la creazione di un modello pilota per collegare a un unico punto di prelievo e consegna energetica un intero condominio, per come entrambi (potenzialmente) correlati al Sistema elettrico (su cui si rinvia *supra*). In tale contesto può inserirsi, tra l'altro, una piattaforma (allo stato, in fase di sviluppo) per la gestione della comunità energetica con l'analisi dei flussi energetici, che si avvale della tecnologia *blockchain* per registrare l'autoconsumo e per implementare gli *smart contracts*, con cui suddividere i ricavi in modo automatico tra i membri.
I dati oggetto del trattamento sono i seguenti:
Dati di registrazione alla piattaforma LEC su cui viene proposto il servizio, dove l'anagrafica di registrazione include nome, cognome, indirizzo, città, provincia, e-mail e codice fiscale.
Dati sull'utenza dell'interessato: numero POD, fornitore delle letture degli *smart meter*s, data di prima attivazione, cabina di media/bassa tensione di afferenza.

Dati energetici della singola utenza su base quartoraria (consumo ed eventuale produzione, ad esempio da pannelli fotovoltaici o accumulo).
Dati impiantistici dell'utenza: potenza impegnata, presenza pompe di calore, accumulo, impianto fotovoltaico, inclusa la geolocalizzaione delle apparecchiature e il loro stato (funzionante/sospeso/errore/non installato).
Sulla base delle informazioni sussistenti allo stato attuale dello sviluppo della piattaforma è emerso che il **titolare** del trattamento dati è ENEA; si segnala, però, che ENEA riceve i dati, da utilizzare a fini di ricerca, dalla **società proprietaria della strumentazione** che rileva/acquisisce i dati di consumo presso le singole utenze.
Il trattamento dei dati coinvolge, inoltre, ulteriori soggetti, ossia: l'amministratore della piattaforma web, l'amministratore della comunità, i ricercatori impegnati su algoritmi, il gestore *token economy* (include *blockchain*). A differenza del "Caso C", tuttavia, il trattamento dati in esame comporta il coinvolgimento anche dell'amministratore della comunità energetica.
L'archivio dati si trova in un database *on-premises*, interno alla rete ENEA, accessibile dall'esterno solo attraverso accessi controllati e ristretti al minimo necessario per la funzionalità del servizio (via WEB e via APP).
La struttura del *database* è compartimentata con logiche di sicurezza in modo da impedire accessi non strettamente funzionali agli obiettivi del servizio.
I dati personali anagrafici sono oggetto di *storage* dedicato separato. I dati sono pseudoanonimizzati (su due differenti *databases* con chiave di relazione) in modo da impedirne la riconducibilità diretta al soggetto. Il dato gestito in *blockchain* è, infatti, su un *database* differente rispetto ai dati di anagrafica, per evitare l'immediata riconducibilità all'interessato; esiste poi un codice che mette in relazione le due tabelle e le relative informazioni.
La conservazione dei dati anagrafici avverrà per la durata del progetto (2021) e per 12 mesi dopo la fine del suo *follow-up* (2022-24) ai fini di ricerca.
Dal momento che nella fattispecie convergono due casi già trattati, si rinvia *supra*, alle considerazioni sviluppate in precedenza sub A e DC.

2.14 *Caso E – Piattaforma* software *in grado di monitorare i* social media web *per estrarre informazioni sulle comunità energetiche*

L'ultimo caso riguarda una piattaforma di gestione e di elaborazione di grandi dati finalizzata all'esecuzione sincrona di applicativi interoperabili su diverse piattaforme per l'acquisizione e l'elaborazione di dati (*crowdsourcing*) provenienti dai *media* e dai *social network* (in particolare Twitter). Per l'acquisizione dei dati e la loro classificazione sono previsti un'ontologia del dominio "*Energy Community*" e un *web-crawling*, con un filtro semantico a essa correlato.
La finalità del software è quella di estrarre informazioni sulle comunità energetiche.
Tenuto conto della nozione ampia di dato personale (che, come già evidenziato, ai sensi dell'art. 4 GDPR, consiste in "qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente (…)") i dati acquisiti da testi scritti su Twitter e da articoli di giornale on-line, corredati delle informazioni legate alla provenienza, eventualmente al nickname o nome reale della persona scrivente ed alla data, dovrebbero essere trattati come dati personali.
Di conseguenza, il loro trattamento (oltre ad avere una legittima base giuridica) dovrebbe avvenire nel rispetto di tutti i principi del GDPR sopra menzionati (e di cui occorre dare dimostrazione, ad es. con registro del trattamento, valutazione impatto privacy, ecc.).
Si suggerisce, dunque, di avvalersi di tecniche di anonimizzazione in modo tale che non sia possibile nemmeno ai tecnici/ricercatori ENEA risalire ai dati personali eventualmente raccolti ed elaborati (come ad es. il *nickname* dell'utente del *social network*).
Come già evidenziato, infatti, l'anonimizzazione è una tecnica che consente di sottrarre l'informazione acquisita al GDPR.

3 Conclusioni

La ricerca ha dato conto delle principali questioni derivanti dalle applicazioni concrete del GDPR nella sperimentazione delle nuove comunità energetiche.
Delineato il quadro normativo di riferimento, si è tentato di tracciare un "percorso guidato" per la protezione dei dati personali nell'ambito di progetti connessi alle comunità energetiche di nuova sperimentazione.
A tale fine, sono stati indicati gli *steps* principali da seguire per una piena *compliance* dei progetti alla disciplina in tema di dati personali.
Il "*vademecum*" è affiancato da un'apposita *flowchart* (che si allega) per agevolare chi è impegnato nello svolgimento di attività relative alle operazioni di trattamento dei dati personali nell'ambito delle comunità energetiche a orientarsi nella normativa in tema di *privacy* e a considerarne le implicazioni, fin dal momento della progettazione.
La correlata (e allegata) *check list*, funzionale ad affrontare i singoli casi d'uso, di cui si è dato conto, potrebbe costituire un primo strumento per mettere in comunicazione i tecnici/ricercatori e il DPO, oltre che per agevolarne e semplificarne uno scambio di informazioni, già nella fase embrionale delle sperimentazioni.
In vista di ulteriori sviluppi della ricerca, si suggerisce, innanzitutto, di consultare le Regole deontologiche per trattamenti a fini statistici o di ricerca scientifica pubblicate ai sensi dell'art. 20, comma 4, del d.lgs. 10 agosto 2018, n. 101 - 19 dicembre 2018, pubblicate dal Garante della Privacy.
Al contempo, si evidenzia l'opportunità di considerare gli allegati elaborati (*flowcharts*, *check list*), tenuto conto del "*vademecum*" sopra riportato, per valutare, in prima battuta, se la sperimentazione che si intende porre in essere potrebbe coinvolgere dati personali e comprendere gli accorgimenti da adottare per la realizzazione di modelli conformi alla normativa di riferimento.
In via generale si segnalano i seguenti "*alerts*":
1) la nozione di dato personale è piuttosto ampia (si v. *supra*, step 1). I dati personali non sono solo i dati sensibili (che, come indicato, sono un "sottoinsieme" di un *genus* più esteso), ma - in via di prima approssimazione – i dati identificativi di una persona fisica.
Ad esempio, con specifico riferimento ai contatori intelligenti, si ribadisce che possono essere considerati oggetto di trattamento i seguenti dati:

• "codice identificativo univoco del contatore intelligente e/o numero di riferimento univoco dell'immobile (in mancanza di tali elementi identificativi, il contatore può comunque essere identificato mediante il suo grafico specifico del carico energetico);

• metadati relativi alla configurazione del contatore intelligente;

• descrizione del messaggio che viene trasmesso, per esempio se si tratta di una lettura del contatore o di una segnalazione di manomissione;

• indicazione di data e ora;

• contenuto del messaggio".

Ai nostri fini, occorre evidenziare che tra le ipotesi di liceità del trattamento delle "particolari categorie di dati" (il sottoinsieme del *genus* più ampio al quale ci si riferiva *supra*) vi è quella legata alla ricerca scientifica (seppur alle condizioni specificate dal citato art. 9, par. 2, lett. j), del GDPR).

2) Occorre poi prestare particolare attenzione al concetto di anonimizzazione dei dati. Al riguardo, pare opportuno ricordare l'ultima parte del Considerando 26 del GDPR, secondo cui "i principi di protezione dei dati non dovrebbero […] applicarsi a informazioni anonime, vale a dire informazioni che non si riferiscono a una persona fisica identificata o identificabile o a dati personali resi sufficientemente anonimi da impedire o da non consentire più l'identificazione dell'interessato".
Occorre considerare, dunque, che si ha anonimizzazione esclusivamente quando il titolare non è in grado, in alcun modo, di re-identificare l'interessato. Solo in presenza di una tecnica di questo tipo, l'informazione acquisita è sottratta al GDPR. Ad esempio, quando, prima della condivisione al soggetto ricevente, il riferimento identificativo del punto di connessione dell'interessato alla rete elettrica (POD) è sostituito da un codice numerico che solo il DSO (contitolare del trattamento) è in grado di associare al cliente (e che ne

consente, dunque, la re-identificazione) sembra esserci anonimizzazione, al più, peril ricevente, ma non per il Distributore.
3) Occorre ricordare l'esigenza di un registro di trattamento dati (su cui si v. *supra*), per ciascuna delle sperimentazioni legate alle comunità energetiche, qualora siano trattati dati personali.
4) Occorre garantire i diritti individuati dal GDPR (e la *compliance* alla relativa disciplina anche in caso di nuove tecnologie, come la *blockchain*, adottando appositi accorgimenti, su cui si v. *supra*).
5) Occorre delineare puntualmente i vari compiti spettanti a tutti i soggetti coinvolti nella sperimentazione e che entrano in contatto, in vario modo, con dati personali, per agevolare l'individuazione dei diversi ruoli e responsabilità.
6) Occorre considerare che, poiché le sperimentazioni in atto coinvolgono per lo più o trattamenti su larga scala o decisioni basate su trattamenti automatizzati (inclusa la profilazione), è necessaria una VPIA (su cui si v. *supra*).
7) Sembra affermarsi in giurisprudenza che, in caso di impiego di un algoritmo, il consenso dell'interessato non sia validamente prestato nel caso in cui lo schema esecutivo dell'algoritmo e gli elementi di cui si compone restino ignoti o non conoscibili da parte degli interessati. Occorre tenere considerazione di tale orientamento nella predisposizione dei moduli di consenso.
8) Nel caso in cui la sperimentazione, per la quale è stato prestato il consenso dell'interessato, muti (ad es., attraverso l'impiego di nuove tecnologie) occorre aggiornare l'informativa prima di procedere.
9) Si ricorda che la *compliance* al GDPR riguarda tutte le ipotesi di trattamento di dati personali emergenti in un contesto di comunità energetiche (non solo quelle legate ai progetti ENEA). L'individuazione delle questioni principali prospettate in questo studio potranno essere di ausilio, dunque, anche per altre comunità energetiche. A tale fine, pare utile rammentare che, ai sensi dell'art. 37 GDPR, in ambito privato, la nomina di un DPO è obbligatoria quando il titolare effettua, nel contesto delle proprie "attività principali": i) trattamenti che comportano il "monitoraggio regolare e sistematico" degli interessati su larga scala; ii) trattamenti "su larga scala" di categorie particolari di dati personali di cui all'art. 9 (dati particolari), o di dati relativi a condanne penali e a reati di cui all'art. 10 GDPR.

4 Allegati

4.1 Check list e diagramma

1. Il progetto coinvolge/potrebbe coinvolgere dati personali?

- ☐ Si
- ☐ No

Il dato personale consiste in qualsiasi informazione riguardante una persona fisica identificata o identificabile, anche indirettamente (art. 4, Regolamento sulla protezione dei dati personali).

A titolo meramente esemplificativo, si considerino i:

i) dati identificativi o anagrafici, ossia nome, cognome, indirizzo e-mail, numero di telefono, codice fiscale, ragione sociale, ecc.;

ii) dati di contatto e di navigazione/dati identificativi dell'utente, come, ad esempio, il nome dell'*Internet Service Provider* e l'indirizzo del Protocollo Internet (IP), la data e l'ora della richiesta, il codice numerico indicante la risposta fornita dal server, contenuto dei messaggi inviati, altri dati forniti durante le comunicazioni – anche telefoniche – intercorse.

iii) dati forniti volontariamente dall'utente – informazioni identificative – per l'accesso ai servizi offerti tramite sito web/piattaforma, da individuare in apposite informative.

iv) dati contrattuali, ossia i dati necessari per la stipulazione e per l'esecuzione di contratti per lo scambio di beni e di servizi nell'ambito di un *marketplace* (concernenti, ad esempio, informazioni che riguardano il sottoscrittore, il beneficiario del servizio o il destinatario della consegna del bene, come il numero della carta di credito o l'indirizzo della sua casa).

v) dati di consumo, ossia i dati relativi alla fornitura e ai livelli di consumo registrati, raccolti ed elaborati (in particolare, dati di consumo elettrico in un intervallo di tempo espressi in kWh), con l'avvertenza che più brevi sono gli intervalli di misurazione, maggiori saranno i dettagli sul profilo di consumo (e, dunque, dell'utente).

vi) dati storici di fatturazione o quelli del profilo temporale di prelievo.

In caso di risposta affermativa, la disciplina in materia di protezione dei dati personali è applicabile.

Proseguire in caso di risposta positiva o di minimo dubbio

2. Il trattamento è circoscritto ai dati personali strettamente necessari per il raggiungimento delle finalità del progetto?

- ☐ Si
- ☐ No

3. Il trattamento dei dati personali è basato sul consenso specifico degli interessati?

- ☐ Si
- ☐ No

In alternativa, specificare su quale altra base legale si fonda il trattamento.

4. In caso di trattamento basato sul consenso, quest'ultimo è revocabile in ogni momento?

- ☐ Si
- ☐ No

5. È possibile adottare tecniche di pseudanonimizzazione?

- ☐ Si
- ☐ No

6. È possibile adottare tecniche di anonimizzazione?

- ☐ Si
- ☐ No

L'anonimizzazione ricorre quando il titolare del trattamento non è in grado, in alcun modo, di re-identificare l'interessato.

7. I dati personali saranno conservati per un periodo di tempo determinato?
   - ☐ Si
   - ☐ No

Specificare puntualmente entro quale periodo saranno conservati e per quale ragione.

8. È stato individuato il luogo di conservazione dei dati personali?
   - ☐ Si
   - ☐ No

Specificare.

9. Sono stati individuati coloro che hanno accesso ai dati personali? Si tratta di persone autorizzate?
   - ☐ Si
   - ☐ No

Specificare di chi si tratta e i rispettivi ruoli.

10. È attivo un sistema di controllo degli accessi agli ambienti in cui sono conservati i dati personali?
    - ☐ Si
    - ☐ No

11. Ho individuato chi determina le finalità e le modalità del trattamento?
    - ☐ Si
    - ☐ No

Specificare chi è il *data controller.*

Si tratta della persona fisica o giuridica, dell'autorità pubblica, del servizio o altro organismo che, singolarmente o insieme ad altri, determina perché e come trattare i dati personali. Vi è una contitolarità del trattamento, dunque, in caso di determinazione congiunta del "perché" e del "come" devono essere trattati i dati personali.

12. Il trattamento non richiede una *Data Protection Impact Assessment*?
    - ☐ Si
    - ☐ No

Il trattamento può comportare un rischio elevato per i diritti e le libertà delle persone interessate (a causa del monitoraggio sistematico dei loro comportamenti, o per il gran numero dei soggetti interessati di cui sono magari trattati dati sensibili, o anche per una combinazione di questi e altri fattori)?

13. È stato predisposto un registro del trattamento dei dati personali?
    - ☐ Si
    - ☐ No

14. Gli interessati hanno possibilità di accedere ai loro dati personali?
    - ☐ Si
    - ☐ No

15. È possibile aggiornare o cancellare i dati personali degli interessati?
    - ☐ Si
    - ☐ No

16. L' interessato può ottenere la portabilità dei suoi dati personali?
    - ☐ Si

☐ No

17. In caso di processo decisionale automatizzato relativo alle persone fisiche (inclusa la profilazione) l'interessato ha la possibilità di opporsi?

☐ Si

☐ No

18. Nell'eventualità di un *data breach*, è stato elaborato un processo di gestione dati personali e di notifica al Garante della Privacy?

☐ Si

☐ No

Il *data beach* è un incidente di sicurezza che coinvolge i dati personali trattati.

Nota Bene: Eventuali risposte negative alle domande da 1 a 17 costituiscono un "*alert*".

Figura 1. Diagramma

5 Riferimenti bibliografici

1. C. Colapietro, “Il diritto alla protezione dei dati personali in un sistema delle fonti multilivello. Il Regolamento UE 2016/679 parametro di legittimità della complessiva normativa italiana sulla privacy”, (2018), pp. 1-140, Esi, Napoli.
2. E. Cusa, “Sviluppo sostenibile, cittadinanza attiva e comunità energetiche”, Orizzonti del diritto commerciale, 2020, p. 77.
3. T. Favaro, “Transizione energetica e amministrazione decentrata”, Giustamm, 2020, p. 5.
4. D. Aquaro, M. Dell’Oste, “Alle comunità delle rinnovabili spinta da 2,2 miliardi nel Pnrr”, in https://ntplusentilocaliedilizia.ilsole24ore.com/art/alle-comunita-rinnovabili-spinta-22-miliardi-pnrr-AEhOYFF [ultimo accesso il 15 dicembre 2021].
5. H. Hijmans, “The GDPR in the enrgy sector”, in https://fsr.eui.eu/the-gdpr-and-the-energy-sector/ [ultimo accesso il 15 dicembre 2021].
6. https://www.garanteprivacy.it/ [ultimo accesso il 15 dicembre 2021].
7. https://www.garanteprivacy.it/regolamentoue/guida-all-applicazione-del-regolamento-europeo-in-materia-di-protezione-dei-dati-personali [ultimo accesso il 15 dicembre 2021].
8. R. D’Orazio, G. Finocchiaro, O. Pollicino, G. Resta, (a cura di), “Codice della Privacy e Data Protection”, (2021), pp. 1-1795, Giuffrè, Milano.
9. R. Panetta, “Privacy is not dead: it’s Hiring!”, in R. Panetta (a cura di), “Circolazione e protezione dei dati personali, tra libertà e regole del mercato”, pp. 14-16, (2019), Giuffré, Milano.
10. M. Mirone, “Il dato personale: cos’è e come trattarlo”, in M. Martorana (a cura di), “GDPR e Decreto Legislativo 101/2018”, pp. 1-10, 2019, Cedam, Padova.
11. https://www.enisa.europa.eu/publications/pseudonymisation-techniques-and-best-practices_it [ultimo accesso il 15 dicembre 2021].
12. https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/controller-processor/what-data-controller-or-data-processor_it [ultimo accesso il 15 dicembre 2021].
13. G. D’Acquisto, M. Naldi, “Big Data e Privacy By Design”, (2018), specie pp. 33-34, Giappichelli, Torino.
14. EU Blockchain Observatory e Forum, 2018.
15. S. Cejka, F. Zeilinger, A. Veseli, M. Holzleitner e M. Stefan, “A blockchain-based privacy-friendly Renewable Energy Community”, in 9th International Conference on Smart Cities and Green ICT Systems (SMARTGREENS), 2020, Prague, Czechia, SCITEPRESS, 2020, pp. 95-103.
16. Redazione, “Le Linee Guida 7/2020 del Comitato europeo sulla protezione dei dati personali sui concetti di Titolare e Responsabile del trattamento nel RGPD: riflessioni critiche e difficoltà applicative”, Diritto e giustizia, 2020.
17. M. Finck, “Blockchains and Data Protection in the European Union”, European Data Protection Law Review, Volume 4 (2018), Issue 1, pp. 17-35.
18. A. D’Ottavio, “Ruoli e funzioni privacy principali ai sensi del regolamento”, in R. Panetta (a cura di), “Circolazione e protezione dei dati personali, tra libertà e regole del mercato”, pp. 143-184, (2019), Giuffré, Milano.
19. D. Cutulo, “Il GDPR non si applica alle persone giuridiche (quasi mai): ecco le conseguenze”, in Agendadigitale.eu, 2019.
20. B. Saetta, “Persone giuridiche e GDPR”, in Protezionedeidatipersonali.it, 2018.
21. https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/application-regulation/do-data-protection-rules-apply-data-about-company_it [ultimo accesso il 15 dicembre 2021].
22. F. Calisai, “I diritti dell’interessato”, in V. Cuffaro, R. D'Orazio, V. Ricciuto (a cura di), “I dati personali nel diritto europeo”, pp. 327-252 (2019), Giapichelli, Torino.
23. https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/legal-grounds-processing-data/grounds-processing/when-consent-valid_it [ultimo accesso il 15 dicembre 2021].

24. F. Machina Grifeo, “Rating reputazionale su internet, algoritmo in chiaro e consenso specifico”, in NTplusDiritto, 2021.
25. B. Saetta, “Profilazione e processi decisionali automatizzati”, in Protezionedatipersonali.it, 2018
26. F. Di Ciommo, Il diritto all’oblio (oblito) nel regolamento Ue 2016/679 sul trattamento dei dati personali, in Il Foro italiano, 9, 2017, 1 ss.; R. Pardolesi, L’ombra del tempo e (il diritto al) l’oblio, in Questione giustizia, 2017, 76.
27. B. Koops, “Forgetting Footprints, Shunning Shadows. A Critical Analysis of the «Right to be forgotten» in Big Data Practice”, in Tilburg Law School Legal Studies Researcher Paper Series, 8, 2012.
28. A. Bunn, The curious case of the right to be forgotten, in Computer Law and Security Review, 2015, 51, p. 336.
29. R. Pardolesi e A. Palmieri, “Diritto all'oblio: il futuro dietro le spalle”, in Foro it., 2014, IV, pp. 317-322.
30. A. Perucci, Elaborazione dei dati e profilazione delle persone, in V. Cuffaro, R. D'orazio, V. Ricciuto (a cura di), “I dati personali nel diritto europeo”, pp. 413-451, (2019), Giapichelli, Torino.
31. R. Torino, “La valutazione d’impatto (Data protection assesment”, in V. Cuffaro, R. D'orazio, V. Ricciuto (a cura di), “I dati personali nel diritto europeo”, pp. 855-877, (2019), Giappichelli, Torino.
32. https://www.garanteprivacy.it/image/image_gallery?uuid=21c655ec-82b7-45af-8027-c7a384b132f6&groupId=10160&t=1508772963481 [ultimo accesso il 15 dicembre 2021].
33. http://www.interlex.it/2testi/autorit/wp248dpia.pdf [ultimo accesso il 15 dicembre 2021].
34. https://www.garanteprivacy.it/regolamentoue/dpia [ultimo accesso il 15 dicembre 2021].
35. https://ec.europa.eu/energy/content/data-protection-impact-assessment-template-smart-grid-and-smart-metering-systems_en?redir=1 [ultimo accesso il 15 dicembre 2021].
36. G. Jesu, “*Policy* per la gestione dei dati personali all’interno di piattaforme informatiche: una formalizzazione”, in Cibersecurity360.it.
37. V. Bellomia, “*Blockchain e smart contract* nell’ordinamento normativo italiano: definizioni e dubbi interpretativi”, in Judicium.it, 10 dicembre 2020.
38. Bundesamt für Sicherheit in der Informationstechnik (BSI), Sicherheit der Blockchain-Technologie, 2018.
39. https://www.agid.gov.it/sites/default/files/repository_files/allegato_4_-_linee_guida_per_la_modellazione_delle_minacce-dlt.pdf [ultimo accesso il 15 dicembre 2021].
40. The European Union blockchain observatory and forum, Blockchain and the GDPR, 2018.
41. L.D. Ibáñez, K. O’Hara, E. Simperl, “On Blockchains and the General Data Protection Regulation”, in EU Blockchain Forum and Observatory, 2018.
42. F. Rampone, “Data Protection in the Blockchain Environment: GDPR is not a Hurdle to Permissionless DLT Solutions”, in Ciberspazio e diritto, vol. 19, n. 61 (3 - 2018), pp. 457-470.
43. P. De Filippi, “The interplay between decentralization and privacy: the case of blockchain technologies”, in Journal of Peer Production, Issue n.7: Alternative Internets», 2016.
44. F. Di Ciommo, “Diritto alla cancellazione, diritto di limitazione del trattamento e diritto all’oblìo”, in V. Cuffaro, R. D'Orazio, V. Ricciuto (a cura di), “I dati personali nel diritto europeo”, pp. 360-361, (2019), Giappichelli, Torino.
45. G. D’Acquisto, “Blockchain e GDPR: verso un approccio basato sul rischio”, in Federalismi.it, 2, (2021), p. 62.
46. https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:52019IE2261&from=EN [ultimo accesso il 15 dicembre 2021].
47. E. Riva Sanseverino, G. Sciumè, P. Gallo, G. Zizzo, “Sovranità sui dati e tecnologia blockchain nel settore energetico”, in Federalismi.it, 2, (2021), pp. 165-166.

6 Abbreviazioni ed acronimi

AGID: Agenzia per l'Italia Digitale
CAD: codice amministrazione digitale (decreto legislativo 7 marzo 2005, n. 82, ss.mm.ii.)
CEC: comunità energetica dei cittadini
CER: comunità di energia rinnovabile
CIE: Carta d'Identità Elettronica
CNS: Carta Nazionale dei Servizi
DLT: *Distributed Ledgers Technology*
DPIA: *Data protection Impact Assessment* (o valutazione d'impatto)
DPO: *Data protection officer* (o Responsabile della Protezione Dati)
DSO: *Distribution System Operator*
GDPR: *General Data Protection* Regulation (Regolamento UE 2016/679)
IoT: *Internet of Things*
LEC: *local token economy*
PEC: posta elettronica certificata
PMI: piccole e medie imprese
POD: *point of delivery*
SPID: Sistema Pubblico di Identità Digitale

Curriculum scientifico del gruppo di lavoro

Giovanna Iacovone

Professore Associato di Diritto Amministrativo, Università della Basilicata. È abilitata alla prima fascia. Insegna Diritto urbanistico e del paesaggio, Legislazione dei Patrimoni culturali, Modelli giuridici per la valorizzazione del territori. È componente del Collegio dei Docenti del Dottorato di Ricerca in Cities and landscapes: architecture, archaeology, cultural heritage, history and resources, Dipartimento DiCEM, Università della Basilicata. Autrice di tre monografie e numerose pubblicazioni, ha partecipato anche come principal investigato a diversi progetti di ricerca nazionali ed europei (PRIN, PON, Erasmus+ - Cattedra Jean Monnet). È impegnata nella ricerca sui temi del paesaggio e dei beni culturali, dell'urbanistica e della pianificazione strategica, del turismo, del ciclo della performance, temi che ha trattato quale relatrice di numerosi convegni, nazionali ed internazionali.

Giordana Strazza

Laureata in Giurisprudenza con lode e menzione accademica e Dottore di ricerca, con lode, in Discipline Giuridiche, presso l'Università degli studi "Roma Tre". Ha ottenuto, all'unanimità, l'abilitazione alle funzioni di professore di seconda fascia in Diritto amministrativo. Avvocato e docente a contratto presso l'Università della Basilicata, dove attualmente è anche assegnista di ricerca. Collabora all'attività didattica presso l'Università degli studi "Roma Tre". Partecipa a progetti di ricerca ed è componente di comitati editoriali di riviste giuridiche.