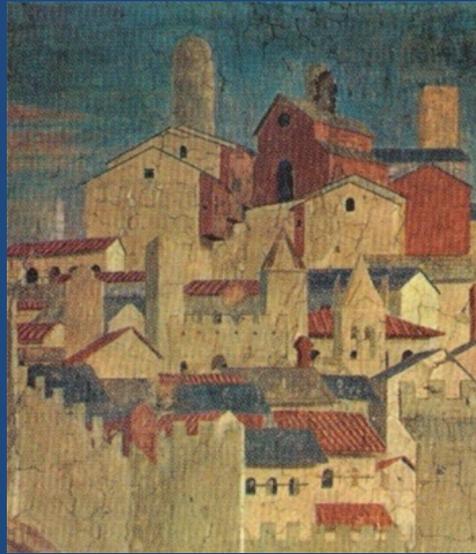


PERSONA E MERCATO



Rivista periodica on-line

www.personaemercato.it

Anno 2023 – Numero 1

ISSN 2239-8570

Persona e Mercato è una rivista fondata da Giuseppe Vettori.

Direzione: Giuseppe Vettori

Comitato di direzione: Fabio Addis; Giuseppina Capaldo; Ernesto Capobianco; Massimo Confortini; Giovanni Di Rosa; Pasquale Femia; Massimo Franzoni; Carlo Granelli; Stefan Grundmann; Francesco Macario; Marisaria Maugeri; Hans W. Micklitz; Emanuela Navarretta; Salvatore Orlando; Fabio Padovini; Stefano Pagliantini; Giovanni Passagnoli; Antonio Rizzi; Pietro Sirena; Massimo Zaccheo.

Comitato dei revisori: Giorgio Afferni; Arianna Alpini; Franco Angeloni; José Luis Argudo Periz; Maria Annunziata Astone; Federico Azzarri; Angelo Barba; Vincenzo Barba; Luca Barchiesi; Andrea Barenghi; Ettore Battelli; Emanuele Bilotti; Lucia Bozzi; Valentina Calderai; Mario Pio Calogero; Simona Caporusso; Gabriele Carapezza Figlia; Valeria Caredda; Roberto Carleo; Sonia Carmignani; Achille Antonio Carrabba; Raffaele Caterina; Guillermo Cerdeira Bravo de Mansilla; Bianca Checchini; Maddalena Cinque; Maria Antonia Ciocia, Claudio Colombo; Nicola Corbo; Alessandra Cordiano; Camilla Crea; Fabrizio Criscuolo; Vincenzo Cuffaro; Alessandro D'Adda; Valeria De Lorenzi; Francesco Delfini; Matteo Della Casa; Stefano Deplano; Francesca Di Lella; Mirko Faccioli; Rocco Favale; Alessia Fachechi; Lourdes Fernandez Del Moral Dominguez; Edoardo Ferrante; Federico Ferro-Luzzi; Nicoletta Ferrucci; Arianna Finessi; Giancarlo Filanti; Massimo Foglia; Luigi Follieri; Giampaolo Frezza; Arianna Fusaro; Francesco Gambino; Rosaria Giampetraglia; Stefania Giova; Cecilia Gomez Salvago Sanchez; Mauro Grondona; Freddy Andrés Hung Gil; Paola Iamiceli; Claudia Irti; Angela La Spina; Eva Leccese; Raffaele Lenzi; Joelle Long; Francesco Longobucco; Emanuele Lucchini Guastalla; Nicola Lucifero; Daniele Maffei; Anna Malomo; Francesca Manolita; Manuela Mantovani; Pierluigi Mazzamuto; Marisa Meli; Raffaella Messinetti; Francesco Mezzanotte; Andrea Mora; Arnaldo Morace Pinelli; Paolo Morozzo della Rocca; Gaetano Edoardo Napoli; Luca Nivarra; Luigi Nonne; Riccardo Omodei Salé; Andrea Orestano; Mauro Orlandi; Mauro Paladini; Massimo Palazzo; Antonio Palmieri; Rosanna Pane; Paolo Papanti Pellettier; Teresa Pasquino; Francesco Paolo Patti; Enza Pellecchia; Mauro Pennasilico; Leonardo Pérez Gallardo; Valerio Pescatore; Mariassunta Piccinni; Carlo Pilia; Fabrizio Piraino; Dianora Poletti; Massimo Proto; Roberto Pucella; Vincenzo Putorti; Maddalena Rabitti; Andrea Renda; Francesco Rende; Giorgio Resta; Francesco Ricci; Vincenzo Ricciuto; Nicola Rizzo; Umberto Roma; Lucia Ruggeri; Antonio Saccoccio; Ugo Salanito; Gabriele Salvi; Giovanna Savorani; Martin Schmidt-Kessel; Anna Scotti; Tommaso Oberdan Scozzafava; Roberto Senigaglia; Anna Maria Siniscalchi; Umberto Stefani; Giovanni Stella; Chiara Tenella Sillani; Giulia Terlizzi; Mauro Tescaro; Stefano Troiano; Alberto Venturelli; Vincenzo Verdicchio; Pietro Virgadamo; Sandra Winkler.

Segreteria di redazione: Daniele Imbruglia e Mario Mauro

Redazione: Francesca Bertelli; Marco Francesco Campagna; Federico Della Negra; Marco Farina; Antonio Gorgoni; Daniele Imbruglia; Antonello Iuliani; Mario Mauro; Tommaso Pellegrini; Federico Pistelli; Chiara Sartoris; Shaira Thobani; Emanuele Tuccari..

E-mail: info@personaemercato.it **Web:** www.personaemercato.it

Persona e Mercato è testata registrata in data 9/10/2000 al n. 4995 dell'elenco della stampa periodica curato dal Tribunale di Firenze.

ISSN 2239-8570

Tutti i diritti di riproduzione sono riservati, comprese le rappresentazioni grafiche ed iconografiche. Ogni riproduzione, anche parziale e qualunque sia il formato e il supporto, è vietata, tranne per uso privato senza alcuno scopo commerciale. Sono consentite, inoltre, le citazioni a titolo di cronaca, studio, critica o recensione. In ogni caso, l'integrità dei documenti riprodotti dovrà essere rispettata e la riproduzione, anche parziale, dovrà essere accompagnata dall'indicazione della fonte.

Tutti i contributi sono stati oggetto di valutazione positiva e anonima da parte di un membro del Comitato dei revisori, ad eccezione dell'Osservatorio a cura dell'OGID, esonerato ai sensi dell'art. 9, V co., del Regolamento per la classificazione delle riviste nelle aree non bibliometriche, approvato con Delibera del Consiglio Direttivo n. 42 del 20.02.2019.

Editoriale

I lividi dei minorenni <i>sparring partners</i> di ChatGPT e l'età minima per attivare il servizio in Italia, di Salvatore Orlando	p. 3
--	------

Saggi

Prescrizione e riduzione, di Mauro Orlandi	p. 7
Appunti sull'art. 2645 <i>quater</i> . Considerazioni dal futuro e questioni dal passato, di Manolita Francesca	p. 20
L'uso delle "tecnologie mobili" applicate alla salute: riflessioni al confine tra la forza del progresso e la vulnerabilità del soggetto anziano, di Claudia Irti	p. 32
NFT and NFTed artworks between property and copyrightability, di Arianna Alpini	p. 50

Commenti

Nota (a margine dell'attuazione della direttiva <i>omnibus</i>) sul potere dell'AGCM di vietare l'utilizzo di clausole vessatorie come pratica commerciale ingannevole, di Salvatore Orlando	p. 61
Fideiussione omnibus ed intesa antitrust: la sentenza delle sezioni unite n. 41994 del 2021, di Enrico Minervini	p. 64
Algoritmo e giustizia alla ricerca di una mite predittività, di Mariano Sciacca	p. 69
<i>Distributed ledger technology</i> e <i>token</i> crittografici. Un "sistema" alternativo di circolazione della ricchezza (e dei diritti?), di Francesco La Fata	p. 85
«Certo, certissimo, anzi probabile»: le alterne e incerte vicende del negozio di accertamento, di Francesco Meglio	p. 99

Osservatorio

Diritto e nuove tecnologie. Rubrica di aggiornamento dell'OGID*	p. 115
---	--------

reputazione non veritiera e produttiva di pregiudizi che possono generare conseguenze ingiustificate o discriminazioni. Rischi destinati ad aumentare se tali trattamenti sono svolti da algoritmi o sistemi di intelligenza artificiale al di fuori di qualunque supervisione umana.

In conclusione, se da un lato questo provvedimento mette in luce una tutela “pratica” e “consumeristica” della protezione dei dati personali, perché a garanzia dell’utente, dall’altro rende evidente perché strutturare il trattamento dei dati personali in modo corretto è molto più di una tutela dell’utente, bensì una tutela della persona e dei suoi spazi di libertà.

Tutela sempre più necessaria in una società governata da sistemi automatizzati che gestiscono ogni aspetto della vita umana: dal suggerimento di contenuti di interesse, all’acquisto di beni e svolgimento di attività sulle piattaforme fino alla possibilità di esercitare diritti o accedere a servizi pubblici.

GUIDO D’IPPOLITO

www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9832979

15. La relazione di ENISA del gennaio 2023 sull’ingegnerizzazione della condivisione dei dati personali con particolare focus sui dati del settore sanitario

Il 27 gennaio 2023 l’ENISA (*European Agency for Cybersecurity*) ha pubblicato il report intitolato “*Engineering Personal Data Sharing - Emerging Use Cases and Technologies*”, riguardante la progettazione di tecnologie e le tecniche specifiche per consentire la condivisione dei dati personali nel pieno rispetto della privacy e del GDPR, in particolare applicato al settore sanitario. Il lavoro è frutto della collaborazione con il gruppo di lavoro *ad hoc* dell’ENISA sull’ingegneria della protezione dei dati personali.

L’Agenzia rileva un aumento della quantità di dati generati, elaborati e successivamente condivisi negli ultimi venti anni, indicando come naturale la tendenza a “portare i dati fuori dai dispositivi o dalle organizzazioni” e a dividerli tra diverse parti per uno scopo specifico al fine di creare nuovo valore per le persone e per la nostra società o semplicemente per ridurre i costi operativi.

Dall’analisi emerge che, considerando solo l’area dei 27 paesi europei, il valore dei dati nel 2025 sarà

di 829 miliardi di euro, rispetto ai 301 miliardi di euro (2,4% PIL dell’UE) del 2018.

Il legislatore europeo è attualmente interessato a sviluppare la potenzialità della condivisione settoriale e intersettoriale dei dati a vantaggio di privati e imprese, mirando a renderli disponibili, anche tramite la regolazione del loro riutilizzo e facilitando questo processo mediante la creazione di nuovi intermediari e di ambienti di condivisione in cui le parti coinvolte possono mettere in comune dati e strutture.

Ottenere e garantire una solida *governance*, nonché tutele efficaci per i diritti delle persone fisiche si rivela essere fondamentale nell’ecosistema di condivisione delle informazioni, in quanto la protezione dei dati personali costituisce la base su cui si fonda la fiducia sia degli individui che delle organizzazioni. Insieme alla regolamentazione, il report individua come centrale il ruolo dell’“ingegneria della protezione dei dati”, strumento adatto a tradurre in concreto i principi della privacy by Design e by Default previsti dall’art. 25 GDPR.

L’ENISA si concentra soprattutto sui casi d’uso nel settore sanitario, sebbene le tecnologie e le tecniche presentate siano ugualmente applicabili anche ad altri ambiti, con l’obiettivo di mostrare come i principi di protezione dei dati possano essere rispettati attraverso l’uso appropriato di soluzioni tecnologiche basate su tecniche crittografiche avanzate. Il settore della salute si presta in modo ottimale a rappresentare il terreno fertile per la condivisione dei dati, rappresentando un’opportunità di sviluppo notevole: il coordinamento e la collaborazione tra gli enti sanitari pubblici e privati, infatti, potrebbe portare a notevoli vantaggi sotto vari profili. A livello istituzionale, la condivisione comporterebbe un generale miglioramento del sistema sanitario, in quanto a livello individuale avrebbe come risultato quello di fornire ai cittadini un’assistenza sanitaria personalizzata ed efficace. Inoltre, a livello collettivo si favorirebbe la conduzione di ricerche scientifiche (compresi gli studi clinici) inerenti la distribuzione nella popolazione di patologie e fattori di rischio e sull’efficacia delle terapie disponibili.

La condivisione, anche transfrontaliera, dei dati sanitari comporta, tuttavia, la necessità di soddisfare i requisiti essenziali del GDPR al fine di ottenere una condivisione che permetta, allo stesso tempo, all’interessato di mantenere un controllo sulle proprie informazioni. I principali obblighi richiesti sono di trasparenza nei confronti dell’utente, in modo che sia sempre consapevole di chi detiene e ha avuto accesso ai suoi dati; di sicurezza e di

minimizzazione. Il report, in particolare, sottolinea la necessità di soddisfare le seguenti proprietà: i dati per la diagnosi e il trattamento dei singoli pazienti devono essere identificabili; quelli per la ricerca medica (eventualmente trattati su larga scala) devono essere adeguatamente pseudonimizzati per garantire che il livello di probabilità di re-identificazione sia ridotto al minimo; deve essere infine presente la capacità di gestire più fonti di dati del paziente, compresi i dispositivi indossabili e le app.

Uno dei case study riportati nel report esplora la situazione di un dispositivo indossabile per il monitoraggio continuo del glucosio (CSM) che, al contempo, monitora anche la pressione sanguigna, i livelli di caffeina e i livelli di lattato 7. Il dispositivo carica i flussi di dati raccolti nel cloud per l'archiviazione e l'ulteriore elaborazione da parte dell'utente stesso e di soggetti terzi, come la sua famiglia e i medici. La complessità principale da superare è quella di permettere all'utente di selezionare specifici flussi di dati da condividere con soggetti specifici e l'ora e il tempo d'accesso, per esempio permettere a un soggetto terzo l'accesso ai dati corrispondenti agli ultimi tre mesi per specifici set di dati. In tal senso, sono descritte alcune soluzioni crittografiche per proteggere la privacy dei dati sanitari durante la loro condivisione tra utenti diversi. In particolare, si tratta di tre tecniche di crittografia asimmetrica: con chiave pubblica, l'Attribute Based Encryption (ABE) e la Proxy Re-encryption. La tecnologia con chiave pubblica prevede che ogni segmento di dati da condividere venga crittografato dall'utente con la chiave pubblica del destinatario interessato. Tale soluzione, tuttavia, risulta poco pratica quando i dati devono essere condivisi tra più entità. L' ABE comporta invece la crittografia dei dati con una chiave pubblica ABE, che consente l'esistenza di più chiavi di decifrazione legate a informazioni aggiuntive relative ai dati, chiamate attributi. La Proxy Re-encryption, infine, consente la condivisione di dati già criptati da una chiave pubblica a un'altra, senza che il proxy abbia accesso al set di dati non criptati.

Uno scenario tipico di condivisione di dati sanitari è quello della gestione delle cartelle cliniche elettroniche (EHR) da parte degli operatori sanitari. Sono cartelle che raccolgono la storia clinica del paziente e di solito vengono conservate in archivi centrali nazionali. Gli utenti possono autorizzare l'accesso ai propri dati ai medici curanti o alle istituzioni mediche. A seguito della pandemia, si è resa urgente la necessità di progetti di raccolta dati ai fini della progressione della ricerca scientifica e della prognosi. Di solito, essendo il sistema

centralizzato, la gestione dei meccanismi di controllo degli accessi viene effettuata dal centro medico, affinché solo i fornitori di servizi sanitari autorizzati abbiano accesso alle informazioni personalizzate. Quando i dati devono essere trasmessi a ricercatori interni o esterni, occorre adottare misure di pseudonimizzazione, al fine di scongiurare l'identificazione del paziente.

ENISA, dunque, propone l'utilizzo della crittografia polimorfica e pseudonimizzazione (PEP), tecnologia che consente di crittografare i dati senza la necessità di stabilire in anticipo chi può decifrarli. Ciò significa che l'accesso ai dati può essere concesso successivamente, a diverse parti con chiavi differenti. Ad ogni individuo viene assegnato uno pseudonimo diverso per ogni richiesta di accesso, quindi ogni paziente ha un identificatore univoco. Questo identificativo viene trasformato in diversi pseudonimi a seconda del destinatario e del contesto della condivisione dei dati. Gli pseudonimi utilizzati per lo stesso paziente non possono essere collegati, preservando così la riservatezza dei dati del paziente. La PEP è già stata testata con successo in uno studio sul morbo di Parkinson e come proposta per il sistema olandese di Electronic Identification (eID).

In conclusione, la condivisione dei dati è un'opportunità di sviluppo notevole per il settore sanitario e per la società in generale, ma deve essere regolamentata adeguatamente per garantire la protezione dei dati personali e la fiducia degli individui e delle organizzazioni. In merito, "l'ingegneria della protezione dei dati" si rivela essere una grande alleata per rispettare i principi di *privacy by design* e *by default* previsti dall'art. 25 GDPR.

CARMINE ANDREA TROVATO

<https://www.enisa.europa.eu/publications/engineering-personal-data-sharing>

16. Il *working paper* dell'ISDA del gennaio 2023 sull'insolvenza nei mercati degli assets digitali

Nel gennaio 2023 l'International Swaps and Derivatives Association ("ISDA") ha pubblicato un *working paper* intitolato "*Navigating Bankruptcy in Digital Asset Markets: Netting and Collateral Enforceability*" vertente sui contratti derivati inerenti ai *digital assets*.

Il documento trae origine dai recenti fallimenti di FTX - nota piattaforma di *trading online* -, "TerraUSD" - una *stablecoin* -, "Three Arrows

