



QUADERNI DEL DIPARTIMENTO DI DIRITTO PUBBLICO  
INTERNAZIONALE E COMUNITARIO

*Nuova serie*

Università degli Studi di Padova

# LA TECNO-SOVRANITÀ NELLA PROSPETTIVA DEL DIRITTO INTERNAZIONALE

*a cura di*

**Andrea Gattini**

€ ??,00



**G. Giappichelli Editore**



QUADERNI DEL DIPARTIMENTO DI DIRITTO PUBBLICO  
INTERNAZIONALE E COMUNITARIO

*Nuova serie*

Università degli Studi di Padova

---



# LA TECNO-SOVRANITÀ NELLA PROSPETTIVA DEL DIRITTO INTERNAZIONALE

*a cura di*

Andrea Gattini



G. Giappichelli Editore

© Copyright 2026 - G. GIAPPICHELLI EDITORE - TORINO

VIA PO 21 - TEL.: 011-81.53.111

<http://www.giappichelli.it>

ISBN/EAN 979-12-211-1931-2

ISBN/EAN 979-12-211-8412-9 (ebook - pdf)

ISBN/EAN 979-12-211-8413-6 (ebook - epub)

*Il volume è pubblicato con il contributo finanziario del Dipartimento di Diritto Pubblico, Internazionale e Comunitario dell'Università di Padova - Unione Europea - Next Generation EU, Missione 4 Componente 1, "Social Cohesion and International Law" (SCIL) - CUP C53D23002940006 – responsabile dell'unità operativa prof. Andrea Gattini.*



*Stampa:* Rotolito S.p.A. - Pioltello (MI)

Le fotocopie per uso personale del lettore possono essere effettuate nei limiti del 15% di ciascun volume/fascicolo di periodico dietro pagamento alla SIAE del compenso previsto dall'art. 68, commi 4 e 5, della legge 22 aprile 1941, n. 633.

Le fotocopie effettuate per finalità di carattere professionale, economico o commerciale o comunque per uso diverso da quello personale possono essere effettuate a seguito di specifica autorizzazione rilasciata da CLEARedi, Centro Licenze e Autorizzazioni per le Riproduzioni Editoriali, Corso di Porta Romana 108, 20122 Milano, e-mail [autorizzazioni@clearedi.org](mailto:autorizzazioni@clearedi.org) e sito web [www.clearedi.org](http://www.clearedi.org).



# INDICE

|               | <i>pag.</i> |
|---------------|-------------|
| <i>Autori</i> | XI          |

## INTRODUZIONE

### TECNOSOVranITÀ E DIRITTO INTERNAZIONALE, UNA SFIDA EPOCALE

ANDREA GATTINI

XIII

## PARTE PRIMA

### IL RUOLO DELLE ORGANIZZAZIONI INTERNAZIONALI

#### LA RICERCA DEL DIRITTO INTERNAZIONALE IN TEMA DI SICUREZZA DIGITALE NELLA PROSPETTIVA DELLE ORGANIZZAZIONI INTERNAZIONALI

PIA ACCONCI

|                                                                                                                                                                                                                                                                                                                                    |    |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----|
| 1. Considerazioni introduttive                                                                                                                                                                                                                                                                                                     | 3  |
| 2. Sicurezza digitale attraverso l'attività delle organizzazioni internazionali                                                                                                                                                                                                                                                    | 6  |
| 3. La sicurezza digitale strumentale al mantenimento della pace e sicurezza internazionale, allo sviluppo sostenibile, alla tutela dei diritti della persona, all'attendibilità dell'informazione, alla stabilità dell'economia di mercato e del commercio internazionale, al tempo della diffusione dell'intelligenza artificiale | 11 |
| 4. Le organizzazioni internazionali regionali di fronte alla diffusione della tecnologia digitale, in particolare dell'intelligenza artificiale                                                                                                                                                                                    | 19 |
| 5. Considerazioni conclusive                                                                                                                                                                                                                                                                                                       | 23 |

LE MINACCE IBRIDE  
ALLA PROVA DEL DIRITTO INTERNAZIONALE  
REBEKKA MONICO

|                                                                                     |    |
|-------------------------------------------------------------------------------------|----|
| 1. Le minacce ibride alla pace e alla sicurezza internazionale: nozione e tipologie | 27 |
| 2. La disinformazione                                                               | 29 |
| 3. Gli attacchi cibernetici                                                         | 35 |
| 4. Il sabotaggio di infrastrutture critiche essenziali sottomarine                  | 40 |
| 5. Considerazioni conclusive                                                        | 47 |

EU TECH REGULATION AND DIGITAL SOVEREIGNTY  
ANTONIO SEGURA-SERRANO

|                                                        |    |
|--------------------------------------------------------|----|
| 1. Introduction                                        | 51 |
| 2. The Digital Services Act and VLOPs/VLOSEs           | 53 |
| 2.1. From the Electronic Commerce Directive to the DSA | 53 |
| 2.2. DSA's Due Diligence Obligations                   | 54 |
| 2.3. DSA's Special Obligation for VLOPs/VLOSEs         | 57 |
| 2.4. DSA's Legal Issues and Assessment                 | 59 |
| 3. The Artificial Intelligence Act (AI Act)            | 62 |
| 3.1. The AI Act's Regulatory Approach                  | 62 |
| 3.2. The AI Act's Weaknesses                           | 65 |
| 4. Concluding Remarks                                  | 67 |

LE NORME TECNICHE INTERNAZIONALI  
TRA TENSIONI E MISURE A TUTELA  
DELLA SOVRANITÀ DIGITALE EUROPEA  
ANNALISA VOLPATO

|                                                                                                             |    |
|-------------------------------------------------------------------------------------------------------------|----|
| 1. Introduzione                                                                                             | 69 |
| 2. Origini e caratteristiche della normazione tecnica internazionale                                        | 72 |
| 3. Il rilievo delle norme tecniche internazionali nel diritto dell'Unione europea                           | 74 |
| 3.1. Il rinvio diretto in atti vincolanti e specifiche tecniche                                             | 74 |
| 3.2. Il rinvio a norme europee ed il c.d. Nuovo Approccio                                                   | 77 |
| 3.3. L'allineamento tra norme tecniche europee ed internazionali                                            | 80 |
| 4. L'evoluzione geopolitica e sociotecnica in tensione con i valori europei                                 | 82 |
| 5. La reazione delle istituzioni europee a tutela dei diritti fondamentali e dei valori dell'Unione europea | 84 |

|                                                                                      | <i>pag.</i> |
|--------------------------------------------------------------------------------------|-------------|
| 5.1. Le modifiche alla procedura di adozione delle norme armonizzate                 | 85          |
| 5.2. L'introduzione di limiti sostanziali all'incorporazione di norme internazionali | 86          |
| 6. Conclusioni                                                                       | 88          |

## IL GDPR NEL QUADRO DELLE INIZIATIVE EUROPEE PER LA SOVRANITÀ DIGITALE ALL'INDOMANI DEL REGOLAMENTO SULL'INTELLIGENZA ARTIFICIALE

CHIARA CELLERINO

|                                                                                     |     |
|-------------------------------------------------------------------------------------|-----|
| 1. Introduzione                                                                     | 91  |
| 2. Il GDPR e gli altri strumenti di regolazione dei mercati digitali: cenni         | 94  |
| 3. L'idoneità del GDPR ad applicarsi alle tecnologie di intelligenza artificiale    | 97  |
| 4. Profili di tensione tra GDPR e tecniche di elaborazione dei c.d. <i>big data</i> | 99  |
| 5. GDPR e Regolamento IA: quale livello di coordinamento normativo?                 | 102 |
| 6. Conclusioni                                                                      | 104 |

## SFIDE E OPPORTUNITÀ NEL RECEPIMENTO DELLA DIRETTIVA DELL'UE SULLE MISURE PER UN LIVELLO COMUNE ELEVATO DI CIBERSICUREZZA (NIS2)

FRANCESCO PAOLO MICOZZI

|                                                                                            |     |
|--------------------------------------------------------------------------------------------|-----|
| 1. Introduzione                                                                            | 107 |
| 2. Sovranità digitale e cyber-resilienza                                                   | 108 |
| 3. La base giuridica dell'azione dell'Unione europea: un caso di <i>competence creep</i> ? | 113 |
| 4. La Direttiva NIS2                                                                       | 117 |
| 5. Il recepimento della Direttiva NIS2 in Italia                                           | 119 |
| 6. Soggetti obbligati e registrazione sul portale ACN                                      | 122 |
| 7. <i>Segue.</i> Misure di <i>cybersecurity</i>                                            | 126 |
| 8. <i>Segue.</i> Incidenti e loro notifica                                                 | 131 |
| 9. <i>Segue.</i> Divulgazione coordinata delle vulnerabilità                               | 134 |
| 10. Conclusione                                                                            | 136 |

PARTE SECONDA  
SOVRANITÀ TECNOLOGICA E DIRITTI INDIVIDUALI

LE INTERFERENZE STRANIERE NEI PROCESSI  
ELETTORALI: PROFILI DI DIRITTO INTERNAZIONALE  
TRA SOVRANITÀ E DIRITTI UMANI

MATTEO SARZO

|                                                                         |     |
|-------------------------------------------------------------------------|-----|
| 1. Introduzione                                                         | 141 |
| 2. Casi recenti di interferenze nelle elezioni attraverso la tecnologia | 143 |
| 3. L'interferenza nelle elezioni e la sovranità                         | 150 |
| 4. L'interferenza nelle elezioni e i diritti umani                      | 155 |
| 5. Conclusioni                                                          | 163 |

L'USO DELL'INTELLIGENZA ARTIFICIALE  
NELLA ATTIVITÀ INVESTIGATIVA

ANTONIO BALSAMO, ANNAMARIA PICOZZI

|                                                                                                                                |     |
|--------------------------------------------------------------------------------------------------------------------------------|-----|
| 1. La rivoluzione digitale e il parallelo sviluppo del <i>cybercrime</i>                                                       | 165 |
| 2. Cybercrime e sistemi di intelligenza artificiale                                                                            | 166 |
| 3. L'intelligenza artificiale da intendere come una concreta alleata nell'analisi dei dati e nella prevenzione dei crimini     | 170 |
| 4. Le potenzialità della intelligenza artificiale: l'analisi predittiva e i suoi possibili utilizzi nelle attività di indagine | 172 |
| 5. L'uso dell'intelligenza artificiale nel contrasto al crimine: limiti etici e normativi                                      | 175 |

LA TRASFORMAZIONE DIGITALE DEL NUOVO  
PARADIGMA INDUSTRIALE. SFIDE E OPPORTUNITÀ  
PER LA SICUREZZA DEI MERCATI INTERNAZIONALI

RICCARDO LEONCINI

|                                                                |     |
|----------------------------------------------------------------|-----|
| 1. Da Adam Smith a Ronald Coase                                | 181 |
| 2. Catene globali e Industria 4.0                              | 184 |
| 3. Industria 4.0 e vulnerabilità                               | 185 |
| 4. La <i>cybersecurity</i> nei moderni sistemi produttivi      | 186 |
| 5. Le catene di approvvigionamento e i loro punti di debolezza | 189 |
| 6. Sicurezza informatica come <i>asset</i> strategico          | 191 |

# IL DIRITTO D'AUTORE ALLA PROVA DELL'INTELLIGENZA ARTIFICIALE GENERATIVA: CRITICITÀ E SOLUZIONI NELLA PROSPETTIVA DEL DIRITTO INTERNAZIONALE

CARLOTTA CERETELLI

|                                                                                                                                                          |     |
|----------------------------------------------------------------------------------------------------------------------------------------------------------|-----|
| 1. Intelligenza artificiale: fenomenologia scientifica e interferenze pratiche con il diritto d'autore                                                   | 195 |
| 2. Diritto d'autore e <i>input</i> ai modelli di intelligenza artificiale                                                                                | 198 |
| 2.1. Il <i>training</i> dei modelli di intelligenza artificiale                                                                                          | 198 |
| 2.1.1. L'interferenza del <i>training</i> con il diritto esclusivo di riproduzione                                                                       | 198 |
| 2.1.2. Il regime delle eccezioni al diritto di riproduzione: dal " <i>fair use</i> " statunitense al " <i>text and data mining</i> " dell'Unione europea | 200 |
| 2.2. Le istruzioni impartite dagli utenti                                                                                                                | 207 |
| 3. Diritto d'autore e <i>output</i> dei modelli di intelligenza artificiale                                                                              | 209 |
| 3.1. La tutela delle opere prodotte dai modelli di intelligenza artificiale                                                                              | 209 |
| 3.1.1. L'attuale impostazione antropocentrica del diritto d'autore e le sue conseguenze                                                                  | 209 |
| 3.1.2. Prospettive di riforma: dall'esperienza britannica alla personalità giuridica per i modelli di intelligenza artificiale                           | 215 |
| 3.2. Quando l'intelligenza artificiale riproduce, manipola o imita opere senza il consenso dell'autore                                                   | 217 |
| 4. Conclusioni                                                                                                                                           | 220 |

# MECCANISMI DI *SCREENING* DEGLI INVESTIMENTI ESTERI FRA SOVRANITÀ TECNOLOGICA E DIRITTO INTERNAZIONALE

MARCO DIMETTO

|                                                                            |     |
|----------------------------------------------------------------------------|-----|
| 1. Introduzione                                                            | 223 |
| 2. I meccanismi di <i>screening</i>                                        | 227 |
| 2.1. La struttura dei meccanismi di <i>screening</i>                       | 228 |
| 2.2. Il funzionamento dei meccanismi di <i>screening</i>                   | 231 |
| 2.3. La disciplina italiana dei <i>golden powers</i>                       | 234 |
| 3. Meccanismi di <i>screening</i> e diritto internazionale pattizio        | 236 |
| 3.1. <i>Screening</i> e trattati commerciali                               | 236 |
| 3.2. <i>Screening</i> e trattati d'investimento                            | 237 |
| 4. Meccanismi di <i>screening</i> e diritto internazionale consuetudinario | 242 |
| 5. Conclusioni                                                             | 247 |

OSSERVAZIONI PRELIMINARI SULL'IMPATTO  
DELLE TECNOLOGIE DI CONTROLLO REMOTO  
SULLA GIURISDIZIONE EXTRATERRITORIALE IN MATERIA  
DI DIRITTI UMANI: IL CASO DEI MIGRANTI VIA MARE

GUSTAVO MINERVINI

|                                                                                                                                                        |     |
|--------------------------------------------------------------------------------------------------------------------------------------------------------|-----|
| 1. Introduzione                                                                                                                                        | 249 |
| 2. La nozione di giurisdizione extraterritoriale e i suoi consolidati modelli applicativi                                                              | 251 |
| 3. Il superamento dei modelli consolidati e l'emersione di un approccio funzionale alla giurisdizione extraterritoriale: il caso dei migranti via mare | 253 |
| 4. Il ricorso a tecnologie di controllo remoto quale forma di esercizio dell'autorità statale                                                          | 260 |
| 5. Riflessioni conclusive                                                                                                                              | 262 |

SOVRANITÀ TECNOLOGICA, DIRITTI FONDAMENTALI  
E DIRITTO INTERNAZIONALE PRIVATO

SARA TONOLO

|                                                                                                                                                                     |     |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----|
| 1. Osservazioni introduttive                                                                                                                                        | 265 |
| 2. La tutela della sovranità tecnologica nei regolamenti dell'UE                                                                                                    | 269 |
| 3. Le regole unilaterali a tutela della sovranità tecnologica dell'Unione europea e la loro interrelazione con altre disposizioni di diritto internazionale privato | 270 |
| 4. Questioni di giurisdizione                                                                                                                                       | 275 |
| 4.1. Giurisdizione in materia contrattuale                                                                                                                          | 275 |
| 4.2. Giurisdizione in materia di obbligazioni non contrattuali                                                                                                      | 279 |
| 5. Legge applicabile                                                                                                                                                | 284 |
| 6. Osservazioni conclusive                                                                                                                                          | 291 |

## AUTORI

Pia ACCONCI, Professoressa ordinaria di Diritto internazionale presso l'Università degli Studi di Teramo.

Antonio BALSAMO, Presidente della Corte d'Appello di Palermo.

Carlotta CERETELLI, Ricercatrice di Diritto internazionale presso l'Università degli Studi di Padova.

Chiara CELLERINO, Professoressa associata di Diritto dell'Unione Europea presso l'Università degli Studi di Genova.

Marco DIMETTO, Ricercatore di Diritto internazionale presso l'Università degli Studi di Padova.

Andrea GATTINI, Professore ordinario di Diritto internazionale presso l'Università degli Studi di Padova.

Riccardo LEONCINI, Professore ordinario di Economia Politica presso l'Alma Mater Studiorum – Università di Bologna.

Francesco Paolo MICOZZI, Dottore di Ricerca, già Professore a contratto presso l'Università degli Studi di Perugia.

Gustavo MINERVINI, Ricercatore di Diritto internazionale presso l'Università degli Studi di Torino.

Rebekka MONICO, Ricercatrice di Diritto internazionale presso l'Università degli Studi dell'Insubria.

Anna Maria PICOZZI, Sostituto procuratore generale presso la Corte d'Appello di Palermo.

Matteo SARZO, Professore associato di Diritto internazionale presso l'Università degli Studi di Padova.

Antonio SEGURA-SERRANO, Professore ordinario presso l'Università di Granada.

Sara TONOLO, Professoressa ordinaria di Diritto internazionale presso l'Università degli Studi di Padova.

Annalisa VOLPATO, Professoressa associata di Diritto dell'Unione Europea presso l'Università degli Studi di Padova.

# SOVRANITÀ TECNOLOGICA, DIRITTI FONDAMENTALI E DIRITTO INTERNAZIONALE PRIVATO

SARA TONOLO

SOMMARIO: 1. Osservazioni introduttive. – 2. La tutela della sovranità tecnologica nei regolamenti dell'UE. – 3. Le regole unilaterali a tutela della sovranità tecnologica dell'Unione europea e la loro interrelazione con altre disposizioni di diritto internazionale privato. – 4. Questioni di giurisdizione. – 4.1. Giurisdizione in materia contrattuale. – 4.2. Giurisdizione in materia di obbligazioni non contrattuali. – 5. Legge applicabile. – 6. Osservazioni conclusive.

## 1. Osservazioni introduttive

L'evoluzione tecnologica, che stimola le riflessioni in merito alle competenze, alle regole e ai limiti degli Stati in tale ambito, coinvolge pienamente il diritto internazionale privato, dato che, come ben noto, l'avvento di internet e la diffusione della tecnologia ha inciso in maniera significativa anche sulle relazioni internazionali privatistiche, con evidenti implicazioni nel campo dei diritti fondamentali<sup>1</sup>.

Si pensi solo alle questioni interpretative dei contratti conclusi *online* da consumatori, che hanno suscitato le riflessioni della Corte di giustizia dell'Unione europea sulla nozione di “atti compiuti nel paese del consumatore” (condizione per l'applicazione delle regole giurisdizionali vigenti in materia), rispetto all'accessibilità *online* del sito di vendita del produttore<sup>2</sup>, o ai dubbi che potrebbero sorgere

---

<sup>1</sup> L.A. CALVO CARAVAÇA, J. CARRASCOSA GONZALEZ, *Conflictos de leyes y conflictos de jurisdicción en Internet*, Madrid, Colex, 2001.

<sup>2</sup> Corte di Giustizia UE, 7 dicembre 2010, in cause riunite C-585/08 e C-144/09, *Pammer*, ECLI:EU:C:2010:740. Si v. sul punto: M. BOGDAN, *Website Accessibility as a Basis for Jurisdiction under Art. 15 (1) (c) of Brussels I Regulation: Case Note on the ECJ Judgments Pammer and Alpenhof*, in *Yearbook of Private International Law*, 2010, p. 565 ss.; D. SVANTESSON, *Pammer and Hotel Alpenhof – ECJ Decision Creates further Uncertainty about when E-business “Direct Activities” to a Consumer’s State under the Brussels I Regulation*, in *Computer Law & Security Review*, 2011, p. 298 ss.;

rispetto alla trascrivibilità del matrimonio concluso via Zoom tra cittadini italiani con un celebrante dello Stato della California. La Cassazione, come noto, ha affermato la trascrivibilità di un matrimonio celebrato al telefono tra due cittadini pakistani, dei quali però almeno uno si trovi alla presenza del celebrante, in conformità a quanto prevede l'art. 28 della l. n. 218/1995 in merito alla forma del matrimonio, da valutarsi alternativamente in base alla legge del luogo di celebrazione o in base alla legge nazionale di almeno uno dei nubendi<sup>3</sup>; ove le leggi nazionali lo prevedano, si può immaginare che il diritto internazionale privato consenta di affermare la validità di un matrimonio virtualmente celebrato tra persone localizzate fisicamente in Paesi diversi, tramite le tecnologie.

Si tratta di un ambito disciplinare nuovo, complesso, transnazionale per natura<sup>4</sup>, caratterizzato da una costante evoluzione, entro la quale gli Stati adottano regole e procedure diverse, volte a salvaguardare le proprie prerogative digitali, che incidono inevitabilmente sui diritti fondamentali degli individui e delle loro relazioni interpersonali, suscettibili di potenziali valutazioni differenti a seconda della giurisdizione investita della questione che le coinvolge. Si pensi ad es. alla nota giurisprudenza relativa al caso della vendita online – su *Yahoo! France* – di oggetti nazisti, censurata in Francia sulla base del divieto ivi vigente della circolazione di tali oggetti sul territorio dello Stato, e negli Stati Uniti, per effetto dell'adeguamento spontaneo di *Yahoo! Inc.* all'ordinanza francese, non escludendosi tuttavia, ad opera della Corte federale di San Josè e della Corte d'Appello di San Francisco la giurisdizione statale, da verificarsi in base ai collegamenti delle vittime col territorio dello Stato in cui veniva fatta valere la violazione (nel caso peraltro su iniziativa di *Yahoo! Inc.*, che in un primo tempo aveva cercato di prevenire l'esecuzione dell'ordinanza francese che ne sanzionava la condotta per la mancata cancellazione della pagina lesiva dell'art. 645-2 del codice penale francese)<sup>5</sup>.

Nell'ambito di tale analisi, mette conto rilevare come sia attualmente in corso un'ampia codificazione della disciplina da parte dell'Unione europea, che mira ad esercitare la propria sovranità digitale e utilizza il diritto quale strumento rivolto a

---

C. BISPING, *Mandatorily Protected: The Consumer in the European Conflict of Laws*, in *European Review of Private Law*, 2014, p. 513 ss.

<sup>3</sup> Cass., sez. I civile, 25 luglio 2016, n. 15343, in *EIUS*, 2016, p. 330.

<sup>4</sup> C. KESSEDIAN, *Electronic Data Interchange, Internet and Electronic Commerce*, Preliminary Document, no. 7 of April 2000, Hague Conference of Private International Law.

<sup>5</sup> *Yahoo! Inc. v. La Ligue contre le Racisme*, 169 FSupp. 2d 1181 (ND Cal.2001); *Yahoo! Inc. v. La Ligue contre le Racisme*, 433 F3d 1199 (9th Cir.2006) sul punto C.T. MURPHY, *International Law and the Internet: An Ill-Suited Match (Case Note on UEJF & LICRA v. Yahoo! Inc.)*, in *Hastings International and Comparative Law Review*, 2002, p. 405; M.H. GREENBERG, *A return to Lilliput: the LICRA v. Yahoo! Case and the Regulation of Online Content in the World Market*, in *Berkeley Technology Law Journal*, 2003, p. 1191 ss.; P. KINSCH, *Droits de l'homme, droits fondamentaux et droit international privé*, in *Recueil des Cours*, 2005 (318), pp. 9-332, a p. 239 ss.

tale obiettivo. In tale contesto, occorre considerare l'utilità del diritto internazionale privato per risolvere questioni di difficile localizzazione, non ancora regolate in maniera uniforme e concernenti il settore specifico del *Fintech* (c.d. tecnofinanza o tecnologia finanziaria) <sup>6</sup>.

Si pensi ad es. ai casi connessi all'impiego di *blockchain*, la tecnologia che può essere utilizzata in molti settori, assicurando la gestione sicura e decentralizzata delle informazioni, o delle transazioni. Difficile localizzare gli effetti dell'impiego di tale tecnologia perché i nodi possono essere distribuiti in più paesi. Tecnologica è la via di accesso dei singoli a tali sistemi, dal momento che i diritti sui rapporti costituiti tramite *blockchain* sono inseriti in un *token* – un insieme di informazioni digitali registrate su una *blockchain* in grado di conferire un diritto ad un soggetto <sup>7</sup> – ovvero uno strumento informatico ricognitivo di una posizione giuridica su di un bene o su un rapporto obbligatorio emesso dal soggetto passivo a fronte di un apporto avente valore economico, e che consente al soggetto attivo di esercitare uno o più diritti nei confronti dell'emittente <sup>8</sup>. Appare dunque complesso individuare la legge applicabile e il giudice competente ai contratti conclusi tramite *blockchain* – i c.d. *smart contracts* – tramite indizi di collegamento propri della fattispecie, anche se non vi è dubbio che la tecnologia non possa incidere sulla qualificazione contrattuale del rapporto, e non solo nelle ipotesi in cui lo *smart contract* sia posto in essere per dare esecuzione a un'obbligazione già esistente <sup>9</sup>.

L'interrelazione tra evoluzione tecnologica, diritto internazionale privato e sovranità potrebbe tendere a delocalizzare virtualmente le fattispecie da disciplinare, o rispetto alle quali individuare il giudice competente, con un conseguente maggiore rilievo dei criteri di collegamento soggettivi, ovvero domicilio, residenza e cittadinanza delle parti del rapporto, rispetto a quelli inerenti all'oggetto della fattispecie <sup>10</sup>.

---

<sup>6</sup> Per *Fintech* si intende l'insieme delle componenti digitali presenti nel sistema finanziario, che concorrono alla produzione di un servizio o di una relazione finanziaria e che caratterizzano un rapporto obbligatorio sul piano della sua costituzione, dell'oggetto, dell'esecuzione, documentazione e circolazione. Si v. Commissione europea, Direzione generale della Stabilità finanziaria, dei servizi finanziari e dell'Unione dei mercati dei capitali, *Summary Report of the Targeted Consultation on the Review of the Directive on Financial Collateral Arrangements*, FISMA.C.2/ATF, 28 giugno 2023, p. 28 ss.

<sup>7</sup> Tribunale di Firenze, sentenza del 19 dicembre 2018 e Tribunale di Firenze, sentenza del 21 gennaio 2019, con nota di D. FAUCEGLIA, *Scambio e deposito di criptovalute: la responsabilità del gestore della piattaforma*, in *Giurisprudenza Italiana*, 2020, p. 2659 ss.

<sup>8</sup> Può rientrare in un *token* la proprietà di un bene, un diritto di credito, azioni, obbligazioni e altri strumenti finanziari; si distinguono generalmente i *payment token*, gli *utility token* e gli *investment token*.

<sup>9</sup> M. EL HARRAK, *Do Smart Contracts Need New Conflict-of-Laws Rules?*, in A. BONOMI, M. LEHMANN, S. LALANI (eds.), *Blockchain and Private International Law*, Leiden, 2023, p. 483 ss.

<sup>10</sup> A. MILLS, *The Law Applicable to Cross-border Defamation on Social Media: Whose Law Governs Free Speech in Facebookistan?*, in *Journal of Media Law*, 2015, consultabile all'indirizzo: <http://dx.doi.org/10.1080/17577632.2015.1055942>.

Rimane tuttavia di fondamentale rilievo la necessità di tutelare i diritti fondamentali, fortemente condizionati dall'evoluzione delle tecnologie.

È in tale contesto che si può indagare il ruolo del diritto internazionale privato come strumento volto a rendere efficace ed effettiva la tutela dei diritti fondamentali.

È innegabile che i diritti umani si pongono in un rapporto circolare con il diritto internazionale privato<sup>11</sup>: da un lato, essi costituiscono la premessa per l'unificazione del diritto internazionale privato, garantendo agli Stati una base di valori comuni su cui costruire le regole uniformi (come accaduto nel quadro della comunitarizzazione del diritto internazionale privato<sup>12</sup>); dall'altro lato, sono le norme del diritto internazionale privato a rappresentare un sicuro riferimento per promuovere la tutela dei diritti umani. Il rapporto tra i due sistemi normativi è complesso e di non facile coordinamento, come dimostra il dibattito tuttora in corso nella dottrina dei vari Paesi sul punto. Si tratta di un dibattito che attraversa tutti gli ambiti della disciplina, anche se con esiti differenti, e con riguardo a obiettivi diversi: ad es. i principi dell'equo processo sono considerati nell'ambito del diritto processuale civile internazionale e nel quadro dell'arbitrato, i diritti dei minori nel quadro del diritto internazionale privato della famiglia<sup>13</sup>. Elemento comune ai diversi ambiti è tuttavia il ruolo del diritto internazionale privato, che si apprezza in quanto strumento interpretativo volto a coordinare le norme nazionali, in vista delle peculiari esigenze di tutela dei diritti dell'uomo e dunque come strumento di supporto allo sviluppo degli stessi<sup>14</sup>.

---

<sup>11</sup> F. SALERNO, *The Identity and Continuity of Personal Status in Contemporary Private International Law*, in *Recueil des Cours*, 2018 (395), p. 39 ss.

<sup>12</sup> F. POCAR, *La comunitarizzazione del diritto internazionale privato, una "European Conflicts of Law Revolution"?*, in *Riv. dir. int. priv. proc.* 2000, p. 873 ss.; C. KREUZER, *La comunitarizzazione del diritto internazionale privato in materia di obbligazioni extracontrattuali ("Roma II")*, in P. PICONE (a cura di), *Diritto internazionale privato e diritto comunitario*, Padova, 2004, p. 421; S. BARIATTI, *La futura disciplina delle obbligazioni non contrattuali nel quadro della comunitarizzazione del diritto internazionale privato*, in *Riv. dir. int. priv. proc.*, 2005, p. 5 ss.; A. BORRÁS, *Le droit international privé communautaire: réalités, problèmes et perspectives d'avenir*, in *Recueil des Cours*, t. 317, 2005, p. 313 ss.; R. LUZZATTO, *Riflessioni sulla c.d. comunitarizzazione del diritto internazionale privato*, in G. VENTURINI, S. BARIATTI (a cura di), *Nuovi strumenti del diritto internazionale privato. Liber Fausto Pocar*, Milano, 2009, p. 613 ss.; H. GAUDEMET-TALLON, *Unité et diversité: quelques mots de droit international privé européen*, in *Mélanges en l'honneur du Professeur J.-M. Jacquet*, Paris, 2013, p. 387 ss.; J. VON HEIN, E. KIENINGER, G. RÜHL (eds.), *How European is European Private International Law?*, Cambridge, 2019.

<sup>13</sup> Sent. 28 ottobre 2010, ricorso n. 1643/06, *Suda c. Repubblica Ceca*; sent. 1° marzo 2016, ricorso n. 41069/12, *Tabbane c. Svizzera*; sent. 2 ottobre 2018, ricorso 40575/10 e 67474/10, *Mutu e Pechstein c. Svizzera*; sent. 28.1.2020, ricorso n. 30226/10, 17880/11, 17887/11, 17891/11, 5506/16, *Ali Riza e a. c. Turchia*; sent. 20 maggio 2021, ricorso n. 5312/11, *BEG S.p.a. c. Italia*.

<sup>14</sup> F. SALERNO, *The Identity and Continuity of Personal Status in Contemporary Private International Law*, cit., p. 35 ss.

## 2. La tutela della sovranità tecnologica nei regolamenti dell'UE

La sovranità tecnologica, ossia la capacità di sviluppare, produrre e mantenere le proprie tecnologie senza dipendere da altre potenze straniere, è un tema ampiamente dibattuto dal punto di vista economico e geopolitico per l'Unione europea. La dipendenza dall'estero in settori nevralgici come l'intelligenza artificiale, la cybersicurezza, lo spazio e la sostenibilità rischia di esporre l'Europa a dinamiche negative in termini di competitività, sicurezza delle catene di approvvigionamento e definizione degli standard internazionali.

Appena insediata come presidente della Commissione Europea, Ursula von der Leyen aveva sottolineato l'urgenza per l'Europa di avere "piena padronanza e proprietà di tecnologie chiave"<sup>15</sup>. Tali obiettivi vengono poi ribaditi anche da Thierry Breton, commissario europeo al mercato interno: "L'Europa non può realizzare la sua transizione digitale e verde senza stabilire una sovranità tecnologica"<sup>16</sup>.

Appare pertanto evidente che le recenti tensioni geopolitiche hanno solo accelerato un processo già in atto, nell'ambito del quale la necessità di una strategia a livello europeo, è attualmente ancora percepita come un'urgenza.

Un altro concetto spesso connesso a quello di sovranità tecnologica è quello di sovranità digitale; tali nozioni sono spesso intese come sinonimi: in realtà si tratta di due principi distinti. Se il primo riguarda soprattutto la capacità di produrre tecnologie, di non essere dipendenti per il loro sviluppo da paesi terzi, che da un momento all'altro possono bloccare le vendite, se non addirittura diventare nemici, la definizione di sovranità digitale riguarda la capacità di un paese di agire in modo indipendente nel mondo digitale. Il riferimento è dunque a ciò che avviene nel cyberspazio, all'uso dei dati, alla profilazione di chi li produce da parte di altri paesi, al controllo delle reti e alla trasmissione di informazioni via internet. La nazionalità delle aziende che raccolgono le maggiori quantità di dati definisce "non solo la forza di un Paese in termini di capacità tecnologiche", ma anche la sua forza "in termini di capacità tecnologiche digitali"<sup>17</sup>.

Nel contesto di tale evoluzione, il diritto sembra voler anticipare i tempi della realizzazione della piena sovranità tecnologica in Europa, affermando, tramite i nuovi Regolamenti, che si adottano regole armonizzate (ad es. sull'accesso equo ai

---

<sup>15</sup> V. comunicazione della Commissione, del 10 marzo 2020, al Parlamento, al Consiglio europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni, Una nuova strategia industriale per l'Europa, COM (2020) 102, p. 4, 15.

<sup>16</sup> Commissione Europea, (2019), *Questionnaire to the Commissioner-Designate for the Internal Market Thierry Breton*, consultabile al seguente indirizzo [https://ec.europa.eu/commission/commissioners/sites/comm-cwt2019/files/commissioner\\_ep\\_hearings/answers-ep-questionnaire-breton.pdf](https://ec.europa.eu/commission/commissioners/sites/comm-cwt2019/files/commissioner_ep_hearings/answers-ep-questionnaire-breton.pdf).

<sup>17</sup> F. CRESPI, S. CARAVELLA, M. MENGHINI, C. SALVATORI, *European Technological Sovereignty: An Emerging Framework for Policy Strategy*, in *InterEconomics*, 2021, pp. 348-354.

dati e al loro utilizzo nonché sull'intelligenza artificiale), che si applicano indipendentemente dal fatto che i destinatari delle stesse siano stabiliti nel territorio dell'Unione, ovvero tramite quelle che tecnicamente si definiscono, nel diritto internazionale privato, norme unilaterali.

### ***3. Le regole unilaterali a tutela della sovranità tecnologica dell'Unione europea e la loro interrelazione con altre disposizioni di diritto internazionale privato***

Nel quadro dell'analisi degli atti normativi adottati dall'Unione europea nell'esercizio della propria sovranità, appare innanzitutto interessante considerare il *Data Act*, che ha costituito un modello di riferimento anche per altri atti normativi<sup>18</sup>, in quanto diretto a rafforzare la sovranità digitale dell'UE, migliorando l'economia dei dati dell'UE e promuovendo il mercato dei dati competitivi. Gli aspetti più significativi al fine di analizzare il rapporto tra sovranità digitale, diritti umani e diritto internazionale privato entro tale atto riguardano, da un lato, la tecnica normativa che segue il c.d. metodo unilateralista, ripreso poi dal regolamento sull'Intelligenza artificiale, c.d. *AI Act*<sup>19</sup>, e, dall'altro lato, il coordinamento con le norme di diritto internazionale privato bilaterali che possono avere un ruolo nelle questioni oggetto del *Data Act*.

I regolamenti adottati nel quadro della c.d. sovranità digitale dell'UE utilizzano ampiamente il metodo unilateralistico, nell'affermare che si applicano – come nel caso del *Data Act* – “ai fabbricanti di prodotti immessi sul mercato dell'Unione e ai fornitori di servizi correlati indipendentemente dal loro luogo di stabilimento di tali fabbricanti e fornitori”, c) ai “titolari dei dati, indipendentemente dal loro luogo di stabilimento, che mettono dati a disposizione dei destinatari di dati nell'Unione”, f) “ai fornitori di servizi di trattamento dei dati, indipendentemente dal loro luogo di stabilimento, che forniscono tali servizi a clienti nell'Unione”.

---

<sup>18</sup> Regolamento (UE), n. 2023/2854 del 13 dicembre 2023 riguardante norme armonizzate sui dati e sul loro utilizzo e che modifica il Regolamento (UE) 2017/2394 e la Direttiva (UE) 2020/1828, in *GUUE* L 2023/2854, del 22 dicembre 2023, applicabile dal 12 settembre 2025, salvo alcune disposizioni che lo diverranno dal 2026 e dal 2027. Sul punto, si v. in generale C. KOHLER, *Conflict of Law Issues in the 2016 Data Protection Regulation of the European Union*, in *Riv. dir. int. priv. proc.*, 2016, p. 653 ss.

<sup>19</sup> Regolamento (UE) 2024/1689 del Parlamento europeo e del Consiglio del 13 giugno 2024 che stabilisce regole armonizzate sull'intelligenza artificiale e modifica i Regolamenti (CE) n. 300/2008, (UE) n. 167/2013, (UE) n. 168/2013, (UE) 2018/858, (UE) 2018/1139 e (UE) 2019/2144 e le Direttive 2014/90/UE, (UE) 2016/797 e (UE) 2020/1828 (regolamento sull'intelligenza artificiale), in *GUUE*, L 2024/1689, del 12 luglio 2024.

Il *Data Act* utilizza quindi una tecnica propria del diritto internazionale privato per definire la propria applicazione extra-territoriale: se i soggetti considerati dal regolamento, gli attori principali del mercato dei dati, si rivolgono verso il territorio dell'Unione europea devono adeguarsi al *Data Act* nella misura in cui le loro attività rientrano in quelle descritte dall'art. 1, par. 3, di tale atto.

Si tratta di una scelta suscettibile di creare conflitti con altri ordinamenti giuridici interessati ad estendere la propria disciplina sulla rete e sul trattamento dei dati, con inevitabili ricadute sui diritti fondamentali degli individui. Si pensi ad es. ad una azione di risarcimento dei danni da responsabilità extracontrattuale, derivante dalla violazione dei diritti di proprietà industriale su una banca dati oggetto di comunicazione a terzi sulla base del *Data Act*, in contrasto con quanto prevede l'art. 1 del regolamento ora in esame. Le norme dallo stesso poste si applicano indipendentemente dalla disciplina della fattispecie (nel caso specifico individuata tramite le disposizioni del Regolamento Roma II<sup>20</sup>), con la conseguenza che se il titolare dei diritti di proprietà industriale agisce dinanzi al giudice di uno Stato membro potrà ricevere la tutela prevista dal *Data Act*, ma difficilmente questa stessa protezione gli verrà riconosciuta dai giudici degli Stati terzi (entro i quali siano stati diffusi i dati). La sentenza pronunciata dal giudice di uno Stato europeo sarà inoltre difficilmente riconoscibile in uno Stato terzo, con evidente compressione del diritto fondamentale di agire in giudizio per vedere tutelati i propri diritti in materia.

In altri casi, possono verificarsi situazioni in cui una richiesta di trasferimento di dati, basata sulla legislazione di un paese terzo, sia in conflitto con l'obbligo di proteggere tali dati a norma del diritto dell'Unione o dello Stato membro pertinente, in particolare per quanto riguarda la tutela dei diritti fondamentali dell'individuo, quali il diritto alla sicurezza e il diritto a un ricorso effettivo, o gli interessi fondamentali di uno Stato membro connessi alla sicurezza nazionale o alla difesa, nonché la tutela dei dati sensibili sotto il profilo commerciale, inclusa la protezione dei segreti commerciali, e la protezione dei diritti di proprietà intellettuale. In assenza di accordi internazionali atti a disciplinare simili questioni, il trasferimento o l'accesso a dati non personali dovrebbero essere consentiti solo se è stato verificato che l'ordinamento giuridico del paese terzo impone che siano indicati i motivi e la proporzionalità della decisione, che la sentenza o decisione abbia carattere specifico e che l'obiezione motivata del destinatario sia sottoposta al riesame da parte di un organo giurisdizionale competente di un paese terzo, cui sia conferito il potere di

---

<sup>20</sup> Regolamento (CE) n. 864/2007 del Parlamento europeo e del Consiglio, dell'11 luglio 2007, sulla legge applicabile alle obbligazioni extracontrattuali (Roma II), in *GUUE* L 199, 31 luglio 2007, p. 40 ss. Su tale regolamento v. *ex multis* A. DICKINSON, *The Rome II Regulation - The Law Applicable to Non Contractual Obligations*, OUP, Oxford, 2009 e nella dottrina italiana P. FRANZINA, *Il regolamento N. 864/2007/CE sulla legge applicabile alle obbligazioni extracontrattuali ("Roma II")*, in *NLCC*, 2008, p. 971 ss.

tenere debitamente conto dei pertinenti interessi giuridici del fornitore di tali dati (come suggerito dal considerando 101 del *Data Act*).

In tal caso, l'approccio unilaterale del *Data Act* può condurre a configurare la tutela dei diritti fondamentali ivi indicati come limite alla circolazione delle sentenze e dei provvedimenti provenienti da Stati terzi, che, a loro volta, prevedono rimedi extraterritoriali. Così è accaduto ad es. nel caso dell'ordine di esibizione, rivolto a Microsoft, per effetto di un mandato statunitense concernente tutte le *email* di un utente, contenute nel *server*, sito in Irlanda; Microsoft tenta di resistere a tale ingiunzione, richiamando la circostanza che il rispetto della stessa avrebbe violato il *Data Act* e il divieto di esportare i dati al di fuori del territorio dell'Unione europea, ma tale aspetto diventa irrilevante per effetto dell'adozione del c.d. *Cloud Act* (*Clarifying Lawful Overseas Use of Data Act*) da parte del Congresso USA, in base al quale si stabilisce che il mandato statunitense all'esibizione dei dati va rispettato a prescindere dai suoi effetti extraterritoriali<sup>21</sup>.

L'approccio unilateralista, proprio degli atti dell'Unione europea in ambito di sovranità tecnologica, apre il campo alla necessità di coordinamento della disciplina posta dagli stessi con le norme di diritto internazionale privato vigenti entro i singoli Stati, siano esse di fonte nazionale o poste da atti dell'Unione europea.

Il Regolamento sull'Intelligenza Artificiale, che si applicherà dal 2 agosto 2026, afferma l'operatività delle regole dallo stesso previste ai fornitori che immettono sul mercato dell'UE sistemi di IA, indipendentemente dal fatto che essi siano localizzati in uno Stato membro o in uno Stato terzo; esso affronta il tema della valutazione di impatto dei sistemi di intelligenza artificiale sulla tutela dei diritti fondamentali all'art. 27, nonché all'art. 77, regolando i poteri delle autorità che tutelano i diritti fondamentali, cui i privati – che lamentano la violazione – possono presentare un reclamo ai sensi dell'art. 85. Rimane sempre possibile l'operatività di norme dell'Unione in materia di protezione dei consumatori e di sicurezza dei prodotti (art. 2, par. 9), nonché l'adozione da parte degli ordinamenti nazionali di norme più favorevoli ai lavoratori a tutela dei loro diritti (art. 2, par. 10). Per tutti gli aspetti non coperti dal Regolamento rilevano i sistemi nazionali di individuazione della legge applicabile alla responsabilità civile.

Si pensi, ad es., al caso in cui, tramite l'algoritmo di *Amazon*, alcune persone siano state indotte ad acquistare prodotti per suicidarsi e i parenti dei defunti richiedano ad *Amazon* il risarcimento dei danni morali<sup>22</sup>. Rileva, in materia, la disciplina del Regolamento Roma II, che richiama in linea generale la legge del luogo ove si è

---

<sup>21</sup> J. DASKAL, *Microsoft Ireland, the CLOUD Act, and International Lawmaking 2.0*, in *Stanford Law Review Online*, 2018, p. 9 ss.; T.F. BRIER JR, *Defining the Limits of Governmental Access to Personal Data Stored in the Cloud: An Analysis and Critique of Microsoft Ireland*, in *Information Policy*, 2017, p. 327.

<sup>22</sup> <https://www.nytimes.com/2022/02/04/technology/amazon-suicide-poison-preservative.html>.

verificato il danno, ma prevede anche una serie di regole di conflitto speciali in materia di danno ambientale, da concorrenza sleale, responsabilità del produttore.

In attesa che si definisca una regola di conflitto *ad hoc* per la responsabilità civile da intelligenza artificiale, si cercherà dunque una soluzione in via interpretativa, tenendo conto dell'impostazione del Regolamento Roma II che dispone regole speciali per alcune categorie di illeciti. Considerando che la legge del luogo ove si è verificato il danno rischia di rendere imprevedibile, per lo sviluppatore di IA, la legge applicabile, si può forse immaginare un temperamento della stessa tramite il richiamo – per analogia con quanto previsto per la responsabilità per danno ambientale – della legge del luogo in cui si è verificato il fatto su richiesta del danneggiato, oppure – per analogia a quanto previsto per la responsabilità per danno da prodotti – secondo il c.d. *market-targeting*, ovvero secondo il metodo, peraltro diffuso nel diritto UE, in base al quale le norme protettive si applicano nel caso in cui il responsabile si sia diretto con atti specifici nel paese della vittima. Tale ultimo criterio presenta però le criticità che sono già state evidenziate in merito alla giurisprudenza della Corte di Lussemburgo a partire dal caso *Pammer*<sup>23</sup>. Occorrerebbe quindi rimodulare tale criterio coerentemente alle peculiarità dello sviluppo dell'IA, considerando da un lato la necessità di tutelare i diritti fondamentali degli individui, dall'altro lo sviluppo dell'IA coerentemente alle evoluzioni della tecnologia.

Anche nel Regolamento sui dati personali il metodo unilateralista lascia scoperti alcuni ambiti della materia. L'art. 1, par. 10, del *Data Act* afferma la possibilità di concludere contratti di condivisione dei dati “volontari e legittimi”, purché conformi ai requisiti del Regolamento. Il considerando n. 9 chiarisce che “salvo che non disponga altrimenti, il regolamento non pregiudica il diritto contrattuale nazionale, ivi comprese le norme sulla formazione, validità ed efficacia di un contratto, o le conseguenze della risoluzione di un contratto”. I contratti sono dunque considerati lo strumento più idoneo a condividere i dati rientranti nell'ambito di applicazione del *Data Act*. Per individuare il diritto applicabile alla formazione, validità o risoluzione del contratto, occorre dunque considerare le norme del Regolamento Roma I<sup>24</sup>. Il diritto nazionale si può applicare, salvo che il regolamento non disponga altrimenti: nel caso in cui un contratto di trasferimento di dati (ad es. da un'impresa costruttrice di veicoli che trasmetta i dati ad una compagnia assicuratrice) preveda, a favore del titolare, un compenso per la cessione dei dati, che sia lecito in base alla

---

<sup>23</sup> Si v. sul punto *supra* il par. 1.

<sup>24</sup> Regolamento (CE) n. 593/2008 del Parlamento europeo e del Consiglio, del 17 giugno 2008, sulla legge applicabile alle obbligazioni contrattuali (Roma I), in *GUUE* L 177 del 4 luglio 2008, pp. 6-16. Sul punto si v. in generale F. SALERNO, P. FRANZINA (a cura di), *Regolamento CE n. 593/2008 del Parlamento europeo e del Consiglio del 17 giugno 2008 sulla legge applicabile alle obbligazioni contrattuali* (“Roma I”), in *Nuove leggi civ. comm.*, 2009; B. HEIDERHOFF, I. QUEIROLO (eds.), *EU and Private International Law: Trending Topics in Contracts, Successions, and Civil Liability*, Editoriale Scientifica, Napoli, 2023.

legge applicabile al contratto, ma risulti invece “discriminatorio e non ragionevole” ai sensi dell’art. 9 *Data Act*, tale compenso non potrà essere corrisposto al titolare dei dati, in ragione della prevalente applicazione di tale ultima norma. Potremmo allora trovarci in presenza, da un lato, di disposizioni di diritto dell’Unione europea, invocabili come limite alla legge scelta dalle parti, di cui all’art. 3, par. 4 del Regolamento Roma I, ove tutti gli elementi del contratto siano localizzati all’interno dell’UE (circostanza difficile da determinare in caso di trasferimento dei dati), o, dall’altro lato, in coerenza con l’impostazione unilateralista del *Data Act*, di norme di applicazione necessaria ai sensi dell’art. 9 del Regolamento Roma I<sup>25</sup>.

Il coordinamento degli atti dell’Unione europea concernenti la c.d. sovranità digitale con le fonti di diritto internazionale privato si profila dunque necessario e complesso, non essendo condivisibile l’orientamento in base al quale occorrerebbe elaborare una c.d. *lex electronica*<sup>26</sup>, al fine di regolare le fattispecie poste in essere tramite l’uso degli strumenti elettronici, ed applicata, ove possibile, da autorità giudiziarie cibernetiche<sup>27</sup>. La ricostruzione di tale disciplina è, allo stato, talmente indefinita, e priva di organicità, da far dubitare della stessa esistenza di regole consolidate nella prassi. Ad es. considerando la c.d. *lex cryptography*, sistema di regole volto a disciplinare i rapporti creati su *blockchain*, non si comprende l’organicità della stessa e la sua autonomia rispetto a un *corpus* di regole da tempo formatesi nella prassi commerciale e riconducibili in linea generale alla c.d. *lex mercatoria*<sup>28</sup>.

Si è infatti generalmente affermato come prevalente l’approccio volto ad individuare nell’applicazione dei tradizionali istituti del diritto internazionale privato la soluzione a tali questioni (*old wine-private international law in new bottles – internet*<sup>29</sup>)<sup>30</sup>.

---

<sup>25</sup> Sulle norme di applicazione necessaria nel regolamento “Roma I” v. A. BONOMI, *Le norme di applicazione necessaria nel regolamento Roma I*, in N. BOSCHIERO (a cura di), *La nuova disciplina comunitaria della legge applicabile ai contratti internazionali*, cit., p. 173 ss.; Z. CRESPI REGHIZZI, *Effetti sui contratti delle misure normative di contenimento dell’epidemia Covid-19: profili di diritto internazionale privato*, in *Dir. comm. int.*, 2020, p. 923 ss.; Z. CRESPI REGHIZZI, *La “presa in considerazione” di norme straniere di applicazione necessaria nel regolamento Roma I*, in *Riv. dir. int. priv. proc.*, 2021, p. 290 ss.

<sup>26</sup> Si v. A. WRIGHT, P. DE FILIPPI, *Decentralized Blockchain Technology and the Rise of Lex Cryptographia*, 2015, consultabile all’indirizzo [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=2580664](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2580664).

<sup>27</sup> S. HAYAKAWA, *Private Law in the Era of Internet*, in J. BASEDOW, T. KONO (a cura di), *Legal Aspects of Globalization*, The Hague, London, Boston, 2000, pp. 27–34; A. MILLS, *The Law Applicable to Cross-border Defamation on Social Media: Whose Law Governs Free Speech in Facebookistan?*, cit.

<sup>28</sup> D. SINDRES, *Is Bitcoin Out of Reach for Private International Law*, in A. BONOMI, M. LEHMANN, S. LALANI (eds.), *Blockchain and Private International Law*, Brill-Nijhoff, Leiden, 2023, p. 81 ss.

<sup>29</sup> P. O’ CALLAGHAN, *Libel on the Internet*, in *Bar Review*, February 2003, pp. 1-2 consultabile all’indirizzo: [http://homepage.eircom.net/~pocbl/articles/Libel\\_on\\_the\\_Internet.pdf](http://homepage.eircom.net/~pocbl/articles/Libel_on_the_Internet.pdf).

<sup>30</sup> J. CARRASCOSA GONZALEZ, *The Internet – Privacy and rights relating to personality*, in *Recueil des Cours*, 2016 (378), pp. 261-486.

I criteri di giurisdizione e di collegamento, attualmente in vigore, tendenzialmente rivolti a situazioni che hanno una forte connessione con il territorio di un determinato Stato, quale ad es. il “luogo in cui l’evento dannoso è avvenuto o può avvenire”<sup>31</sup>, vanno dunque adattati alle fattispecie localizzate nello spazio telematico, entro il quale ad es. la violazione di un diritto della personalità ha una diffusione potenzialmente globale e si amplia così proporzionalmente a tale ultima circostanza l’individuazione del giudice competente e della legge applicabile, rilevando la localizzazione delle azioni in ambiti non territoriali quali quelli dello spazio telematico (*domains, social networks, portali, piattaforme, forums, blogs, ecc.*).

## 4. Questioni di giurisdizione

### 4.1. Giurisdizione in materia contrattuale

Nella complessa opera di coordinamento tra norme di diritto internazionale privato di diversa fonte (europea e nazionale) al fine di regolare le fattispecie che si realizzano nello spazio telematico, rileva il supporto giurisprudenziale volto ad adattare le regole vigenti in ordine alla disciplina di tali fattispecie. Si tratta di un supporto prevalentemente connesso all’operatività delle regole di giurisdizione, ma suscettibile di interessanti ragionamenti anche in merito all’individuazione della legge applicabile<sup>32</sup>.

Si tratterà allora di vedere in che modo la Corte di Lussemburgo interpreterà le disposizioni del Regolamento Bruxelles I *bis*<sup>33</sup>, per fondare la giurisdizione ad es.

---

<sup>31</sup> Si v. sul punto *infra* par. 4.

<sup>32</sup> Si pensi ad es. alle questioni interpretative dei contratti conclusi *online* da consumatori, che hanno condotto la Corte di giustizia UE a interrogarsi sulla nozione di “atti compiuti nel paese del consumatore” rispetto all’accessibilità del sito di vendita del produttore: Corte di Giustizia UE, 7 dicembre 2010, in cause riunite C-585/08 e C-144/09, *Pammer*, cit.; si v. inoltre 6 settembre 2012, in causa C-190/2011 - *Daniela Mühlleitner c. Ahmad Yusufi and Wadat Yusufi*, par. 44, ECLI:EU:C:2012:542; 17 ottobre 2013, causa n. C-218/12, *Lokman Emrek c. Vlado Sabranovic*, par. 15 ss. ECLI:EU:C:2013:666. Sul punto si v. M. BOGDAN, *Website Accessibility as a Basis for Jurisdiction under Art. 15 (1) (c) of Brussels I Regulation*, cit., p. 565 ss.; D. SVANTESSON, *Pammer and Hotel Alpenhof – ECJ Decision Creates further Uncertainty*, cit., p. 298 ss.; C. BISPING, *Mandatorily Protected: The Consumer in the European Conflict of Laws*, cit., p. 513 ss. Per ulteriori indicazioni relative ai contratti dei consumatori conclusi online, si v. Corte di giustizia UE, 30 settembre 2021, in causa C-296/20, *Commerzbank AG c. E. O.*, ECLI:EU:C:2021:784.

<sup>33</sup> Regolamento (UE) n. 1215/2012 del Parlamento europeo e del Consiglio, del 12 dicembre 2012, concernente la competenza giurisdizionale, il riconoscimento e l’esecuzione delle decisioni in materia civile e commerciale (rifusione), in *GUUE* L 351 del 20 dicembre 2012, pp. 1-32. Sul punto si v. in generale F. SALERNO, *Giurisdizione ed efficacia delle decisioni straniere nel Regolamento (UE) n. 1215/2012 (rifusione)*, 4ª ed., Vicenza, 2015, p. 82; ID., *Lezioni di diritto internazionale privato*, 2ª ed., Milano, 2022, p. 111; U. MAGNUS, P. MANKOWSKI, *Brussels I Regulation*, 2<sup>nd</sup> ed., Munich, 2012, p. 436 ss.; F. POCAR, I.

in ordine ad una azione di natura individuale, concernente l'impiego di *blockchain*, la tecnologia che, come si è detto, può essere utilizzata in molti settori, assicurando la gestione sicura e decentralizzata delle informazioni, o delle transazioni. Appare difficile individuare le regole di giurisdizione, in assenza di una chiara qualificazione della fattispecie, soprattutto nel sistema giuridico italiano, attesa la tipicità legale dei titoli di credito al portatore (art. 2004 c.c.). Ciò, anche alla luce del fatto che i protocolli di anonimato, o l'uso di pseudonimi che spesso caratterizzano gli scambi su *blockchain* rendono incerta la localizzazione del convenuto da parte dell'utente che lamenti di aver subito un pregiudizio all'interno di circuiti di monete virtuali, non tralasciando il fatto che l'impossibilità di localizzare beni o eventi digitali che esistono solo sulla rete, possa contrastare l'applicazione in via interpretativa dei criteri di giurisdizione del regolamento Bruxelles I *bis*<sup>34</sup>.

Appare dunque auspicabile, in materia, lo sviluppo del diritto internazionale uniforme sul modello della Convenzione di Vienna del 1980 sulla vendita internazionale di merci<sup>35</sup>.

In attesa di tale evoluzione normativa, sembra probabile che, al fine di individuare la giurisdizione competente in materia di azioni individuali per rapporti costituiti tramite *blockchain*, si segua l'approccio proprio della giurisprudenza *Pammer*<sup>36</sup>, evitando di considerare accessibile il giudice di qualunque paese in cui la persona titolare del *token* si trovi, ma deducendo la necessità di un collegamento effettivo della fattispecie con quell'ordinamento.

Appare probabile anche il delinearsi futuro di un maggiore rilievo applicativo dei criteri di collegamento soggettivi rispetto a quelli inerenti all'oggetto della fattispecie, attesa l'accessibilità dei contratti tramite gli strumenti di cui sono titolari i singoli, più facilmente localizzabili.

Queste considerazioni potrebbero valere, ad es., per definire la giurisdizione relativa ai contratti conclusi tramite *blockchain* alla base di sistemi di pagamento (PayPal), di prenotazioni, di prestito, attraverso un registro digitale che assicura certezza, trasparenza, segretezza (a chi le esegue) delle operazioni, per natura internazionale, in quanto i diversi blocchi della catena possono essere localizzati in Paesi diversi che ne regolano il funzionamento con norme differenti. Si tratta di un settore non ancora regolato dalle norme nazionali ed internazionali, ad eccezione di qualche fonte che regola l'uso di internet nel commercio internazionale e che per la formulazione generale può ritenersi idonea a regolare i c.d. *smart contracts*

---

VIARENGO, F.C. VILLATA (eds.), *Recasting Brussels I*, Padova, 2012; A. TRUNK, N. HATZIMIHAIL (eds.), *EU Civil Procedure Law and Third Countries. Which Way Forward?*, Baden-Baden, 2021, p. 53.

<sup>34</sup> M. LEHMANN, *Crypto-economie et droit international*, in *Recueil des Cours*, 2024 (438), p. 166 ss.

<sup>35</sup> Convenzione delle Nazioni Unite sui contratti di compravendita internazionale di merci, conclusa a Vienna l'11 aprile 1980, entrata in vigore il 1° gennaio 1988 (CISG).

<sup>36</sup> Si v. sul punto *supra* nt. n. 2.

(contratti conclusi tramite *blockchain*). Ad es. l'art. 12 della Convenzione delle Nazioni Unite sull'uso delle comunicazioni elettroniche nei contratti internazionali del 23 novembre 2005<sup>37</sup> prevede la validità di un contratto formato in seguito all'interazione di un sistema automatico ed una persona o in seguito all'interazione di un sistema di messaggi automatici, nell'ambito dei quali non ricorre l'intervento di nessuna persona umana.

In assenza di regole di diritto privato nazionali, è tuttavia difficile definire la giurisdizione, secondo le norme di diritto internazionale privato vigenti, poiché è difficile operare una qualificazione della fattispecie. Si pensi ad es. ad un contratto di trasporto internazionale di merci collegato ad una compravendita; il pagamento si effettua automaticamente, tramite *token*, nel momento in cui la merce arriva a destinazione e di tale circostanza si ha notizia tramite il GPS localizzato sulla merce: si può fare riferimento a tale aspetto come criterio per individuare la giurisdizione in base al Regolamento Bruxelles *Ibis*, analogamente a quanto stabilito in applicazione del Regolamento Bruxelles I<sup>38</sup>, in maniera prevalente rispetto a quanto previsto dalla Convenzione di Vienna del 1980 sulla vendita internazionale di merci (art. 31)<sup>39</sup>.

Si tratta allora di delineare un metodo di approccio generale alle questioni di giurisdizione poste dagli istituti che costituiscono esplicazione della sovranità digitale dei singoli Stati. Al di là delle ipotesi di accordo tra le parti (art. 25), *forum prorogatum* (art. 26) e giurisdizione esclusiva (art. 24), la regola generale (art. 4)

---

<sup>37</sup> Consultabile all'indirizzo: [https://uncitral.un.org/sites/uncitral.un.org/files/media-documents/uncitral/en/19-09103\\_eng.pdf](https://uncitral.un.org/sites/uncitral.un.org/files/media-documents/uncitral/en/19-09103_eng.pdf).

<sup>38</sup> Regolamento (CE) 44/2001 del 22 dicembre 2000, concernente la competenza giurisdizionale, il riconoscimento e l'esecuzione delle decisioni in materia civile e commerciale, in *GUCE*, n. L 12 del 16 gennaio 2001, pp. 1-23. Tale atto, che sostituiva la Convenzione di Bruxelles del 27 settembre 1968, come noto è stato sostituito dal Regolamento Bruxelles I *bis*. Sul punto si v. F. SALERNO, *La Convenzione di Bruxelles del 1968 e la sua revisione*, Padova, 2000; H. GAUDEMET TALLON, *La transformation de la Convention de Bruxelles du 27 septembre 1968 en Règlement du Conseil concernant la compétence judiciaire, la reconnaissance et l'exécution des décisions en matière civile et commerciale*, in *Rev. critique*, 2001, p. 601 ss.; ID., *Compétence et exécution des jugements en Europe: règlement n. 44/2001, Conventions de Bruxelles et Lugano*, Paris, 2002.

<sup>39</sup> Sul punto si v. CGUE, sentenza del 25 febbraio 2010, causa C-381/08, *Car Trim GmbH c. KeySafety Systems Srl*, ECLI: ECLI:EU:C:2010:90, par. 35. Il caso verteva sull'interpretazione dell'art. 5(1)(b) del regolamento Bruxelles I, ma la sua portata può essere certamente estesa all'art. 7(1)(b) del regolamento Bruxelles I *bis*, in quanto lo stesso regolamento Roma I chiarisce, al considerando n. 17, come il termine "compravendita di beni" vada inteso nello stesso senso attribuito all'art. 5(1)(b) del regolamento Bruxelles I, oggi art. 7(1)(b) del regolamento Bruxelles I *bis*. Sul rapporto tra le due norme, cfr. M. REQUEJO ISIDRO, E. WAGNER, M. GARGANTINI, Article 7, in M. REQUEJO ISIDRO (eds.), *Brussels I bis. A Commentary on Regulation (EU) No 1215/2012*, Cheltenham, 2022, p. 101. Per la prevalenza delle regole di giurisdizione del Reg. Bruxelles I sull'art. 31 della Convenzione di Vienna, si v. Cass. civ., sez. un., 26 febbraio 2016, n. 3802.

individua come competente il foro di uno Stato membro dell'UE in cui il convenuto ha il domicilio.

L'art. 7(1) del regolamento Bruxelles I *bis* prevede il criterio speciale del luogo dell'esecuzione dell'obbligazione dedotta in giudizio. Non facile può essere l'adattamento di tali disposizioni alla materia digitale: ad es. relativamente alle controversie in materia di criptovalute, i cui sistemi operativi si servono della crittografia per celare l'identità dei propri utenti, può risultare oneroso identificare e localizzare il convenuto, così come localizzare il luogo di esecuzione dell'obbligazione se essa va adempiuta sulla rete.

Più agevole è la determinazione del foro competente in controversie riguardanti contratti stipulati tra piattaforme o prestatori di servizi inerenti alle criptovalute e utenti, i quali, secondo l'ampia definizione dell'art. 17 del Regolamento Bruxelles I *bis*, tendenzialmente possono rientrare tra i contratti del consumatore, cui si applicano gli artt. 17, 18 e 19 del Regolamento. Per favorire la parte debole del rapporto contrattuale, tali disposizioni consentono al consumatore, in linea di massima, la scelta di agire dinanzi ai giudici dello Stato in cui si trova il proprio domicilio o quello del convenuto. Un'altra questione che potrebbe porsi nell'ambito dei rapporti tra piattaforme e attività simili e utenti/consumatori riguarda la possibilità di azioni collettive, relativamente alle quali occorre anche sempre considerare il contesto generale degli atti dell'Unione europea<sup>40</sup>. Nonostante il regolamento Bruxelles I *bis* non fornisca indicazioni circa tale possibilità, è possibile osservare che la necessità di determinare la giurisdizione in modo separato per ogni domanda e ogni attore sulla base dei criteri speciali di cui agli artt. 7(1) e (2) e 18(1) promuova di fatto la trattazione disgiunta dei procedimenti.

---

<sup>40</sup> Raccomandazione della Commissione, dell'11 giugno 2013, relativa a principi comuni per i meccanismi di ricorso collettivo di natura inibitoria e risarcitoria negli Stati membri che riguardano violazioni di diritti conferiti dalle norme dell'Unione, in *GUUE* L 201 del 26 luglio 2013; Direttiva (UE) 2020/1828 del Parlamento europeo e del Consiglio del 25 novembre 2020 relativa alle azioni rappresentative a tutela degli interessi collettivi dei consumatori e che abroga la Direttiva 2009/22/CE (Testo rilevante ai fini del SEE), in *GUUE* L 409 del 4 dicembre 2020. Sul punto, si v. B. HESS, *A Coherent Approach to European Collective Redress*, in D. FAIRGRIEVE, E. LEIN (eds.), *Extraterritoriality and Collective Redress*, Oxford, 2012, p. 107 ss.; ID., *Collective Redress and the Jurisdictional Model of the Brussels I Regulation*, in A. NUYTS, N. HATZIMIHAIL (eds.), *Cross-Border Class Actions: The European Way*, München, 2014, p. 59 ss.; C. HODGES, *Collective Redress: A Breakthrough or a Damp Squib?*, in *Journal of Consumer Policy*, 2014, p. 67 ss.; A. PATO, *Jurisdiction and Cross-Border Collective Redress: A European Private International Law Perspective*, Oxford, 2019; K. TAKAHASHI, Z. TANG, *Collective Redress*, in P. BEAUMONT, J. HOLLIDAY (eds.), *A Guide to Global Private International Law*, Oxford, 2022. p. 433 ss.

## 4.2. Giurisdizione in materia di obbligazioni non contrattuali

Problemi complessi si possono determinare anche in relazione alle eventuali azioni di responsabilità extracontrattuale nelle questioni inerenti alla sovranità tecnologico-digitale.

Si tratta di una disciplina oggetto di continua evoluzione e, allo stato, ancora condizionata dall'operatività dei criteri di giurisdizione attualmente in vigore, rivolti a situazioni che hanno una forte connessione con il territorio di un determinato Stato, quale ad es. il "luogo in cui l'evento dannoso è avvenuto o può avvenire", evidenziando così le difficoltà di adattare tali criteri allo spazio telematico.

Dal punto di vista dell'individuazione della giurisdizione, rilevano le norme del regolamento Bruxelles I *bis* nell'interpretazione della Corte di giustizia dell'Unione europea, che adotta degli orientamenti non sempre privi di criticità. Si pensi ad es. alla giurisprudenza concernente le azioni per violazione dei diritti fondamentali, ad es. quelle rivolte a garantire un risarcimento civile dei danni alle vittime di violazioni dei diritti della personalità<sup>41</sup>.

Le azioni di risarcimento del danno derivante dalla diffusione di informazioni personali *online*, si propongono secondo quanto prevede l'art. 7, par. 2, del Regolamento Bruxelles I *bis*, dinanzi all'autorità giurisdizionale del luogo in cui l'evento dannoso è avvenuto o può avvenire. Per le violazioni dei diritti della personalità tramite internet, l'applicazione di tale criterio è particolarmente difficile perché si articola in sei momenti consecutivi, rispetto ai quali può rilevare l'individuazione del criterio di giurisdizione: la creazione del contenuto che viola i diritti fondamentali della vittima (lo scatto di una fotografia, o la creazione di un video); il trasferimento del contenuto ad una terza persona (l'invio di una *mail*, l'*upload* del video o della foto in un sito *web*); l'accesso della terza persona al contenuto lesivo (apertura dell'*email* o accesso a un sito *web*); la comprensione del contenuto lesivo da parte della terza persona; le conseguenze della violazione dei diritti della personalità della vittima (la vittima viene licenziata, riceve una domanda giudiziale di divorzio); gli effetti delle conseguenze dirette della violazione dei diritti della personalità (la vittima ha una perdita economica, la vittima si sente umiliata, la vittima si suicida, ecc.)<sup>42</sup>. Ai fini dell'applicazione dell'art. 7, par. 2, del regolamento Bruxelles I *bis*, l'analisi della giurisprudenza comparata ha evidenziato che il riferimento al luogo in cui si è verificata l'azione va riferito al trasferimento del contenuto ad una terza persona,

---

<sup>41</sup> Corte di Giustizia CE, 7 marzo 1995, in causa C-68/93, *Shevill e a.*, EU:C:1995:61. Corte di giustizia UE, 25 ottobre 2011, in cause riunite C-509/09 e C-161/10, *E Date Advertising*, ECLI: ECLI:EU:C:2011:685; Corte di giustizia UE, 17 ottobre 2017, causa C-194/16, *Bolagsupplysningen OÜ e Ingrid Ilsjan c. Svensk Handel AB*, ECLI:EU:C:2017:766.

<sup>42</sup> D.J.B. SVANTESSON, *Private International Law and the Internet*, Alphen aan den Rijn, 2021.

mentre l'evento dannoso si individua con riguardo alla comprensione del contenuto dannoso da parte di una terza persona<sup>43</sup>.

L'applicazione della norma dell'art. 7, par. 2, del Regolamento Bruxelles I *bis* deve peraltro ispirarsi alla giurisprudenza della Corte di giustizia che ha da tempo elaborato tre fondamentali principi in relazione alle diverse tipologie di illecito, che pongono problemi interpretativi quando vengono realizzati tramite internet (c.d. *cyber torts*), ovvero l'illecito extra-contrattuale a distanza, l'illecito complesso, e con danni plurilocalizzati<sup>44</sup>. Rileva, in primo luogo, il principio della piena dicotomia tra azione ed evento o teoria ubiquitaria (*ubiquity rule* o *Ubiquitätsregel*), per la prima volta sancito nel caso *Mines de Potasse*<sup>45</sup>, che attribuisce all'attore, nei casi di illeciti a distanza, la facoltà di scegliere se adire il giudice del luogo del fatto dannoso (*locus actus*) o il giudice del luogo in cui si è verificato il danno (*locus damni*). Per l'illecito complesso viene in considerazione il principio del fatto causale iniziale<sup>46</sup>, in base al quale è dotato di competenza giurisdizionale il giudice del luogo in cui è localizzato l'evento causale iniziale che ha dato origine al danno (se tale fatto è di per sé idoneo a cagionare il danno). Nel caso di danni plurilocalizzati si deve considerare il principio, elaborato sempre nel quadro del caso *Shevill*, del trattamento a mosaico (*mosaic principle*)<sup>47</sup>, in base al quale il giudice del luogo del fatto dannoso è competente a conoscere del risarcimento della totalità dei danni mentre il giudice del luogo del danno è competente per i soli danni cagionati nella circoscrizione del giudice adito. La Corte di giustizia dell'Unione europea ha poi ampliato il principio della dicotomia tra azione e danno, individuando un terzo foro potenzialmente competente, da individuarsi, ad es. in materia di diffamazione *online*, nel centro di interessi della persona fisica diffamata<sup>48</sup>, e nel centro di interessi della persona giuridica diffamata<sup>49</sup>.

Nella sentenza *Shevill*, la Corte di giustizia ha confermato la teoria ubiquitaria, adeguandola a una controversia diffamatoria a mezzo stampa, e ha elaborato il principio del fatto causale iniziale e del trattamento a mosaico. In particolare, la Corte ha

---

<sup>43</sup> J. CARRASCOSA GONZALEZ, *The Internet – Privacy and rights relating to personality*, cit., p. 334.

<sup>44</sup> E. GABELLINI, *La competenza giurisdizionale nel caso di lesione di un diritto della personalità attraverso internet*, in *Riv. trim. dir. proc. civ.*, 2014, p. 271.

<sup>45</sup> Corte di Giustizia CE, 30 novembre 1976, in causa C- 21/1976, *Handelskwekerij G. J. Bier BV v Mines de potasse d'Alsace SA*, ECLI:EU:C:1976:166.

<sup>46</sup> Corte di Giustizia CE, 7 marzo 1995, in causa C-68/93, *Shevill e a.*, cit.

<sup>47</sup> P. FRANZINA, *La giurisdizione in materia contrattuale: l'art. 5 n. 1 del Regolamento n. 44/2001/CE nella prospettiva della armonia delle decisioni*, Padova, 2006, p. 409.

<sup>48</sup> Corte di giustizia UE, 25 ottobre 2011, in cause riunite C-509/09 e C-161/10, *E Date Advertising*, ECLI: ECLI:EU:C:2011:685.

<sup>49</sup> Corte di giustizia UE, 17 ottobre 2017, causa C-194/16, *Bolagsupplysningen OÜ e Ingrid Iksjan c. Svensk Handel AB*, cit., par. 47.

stabilito che sono competenti a conoscere del risarcimento del danno cagionato alla reputazione e alla considerazione di persone fisiche o giuridiche<sup>50</sup> sia i giudici del luogo in cui è stabilito l'editore della pubblicazione diffamatoria in quanto «luogo di origine del fatto dannoso a partire dal quale la diffamazione è stata formulata e messa in circolazione»<sup>51</sup>, sia i giudici del luogo di diffusione della pubblicazione quando la vittima sia ivi conosciuta (luogo del danno). Il giudice in cui è domiciliato l'editore conosce del risarcimento totale o integrale del danno, mentre il giudice del luogo in cui è diffusa la pubblicazione conosce del risarcimento parziale ossia dei soli danni cagionati, in tale Stato, alla reputazione e all'onore della vittima<sup>52</sup>.

Nella sentenza *eDate*, la Corte di giustizia ha adattato i principi interpretativi formulati nel caso *Shevill* alla diffamazione tramite Internet, dal momento che le informazioni divulgate *online* sono immediatamente e universalmente accessibili da un numero potenzialmente indeterminato di utenti in qualunque parte del mondo e in qualsiasi momento (c.d. ubiquità della rete)<sup>53</sup>. La vittima della diffamazione ha dunque la facoltà di scegliere se adire, oltre al foro generale del domicilio del convenuto, quale giudice del luogo del fatto, competente a conoscere del risarcimento integrale del danno subito, il giudice del luogo in cui è stabilito il soggetto che ha messo in rete i contenuti diffamatori o il giudice del luogo in cui si trova il centro di interessi dell'attore stesso, vittima della diffamazione (*forum actoris*)<sup>54</sup>, o quale giudice del luogo del danno, competente a conoscere del risarcimento del solo danno subito sul territorio dello Stato membro del giudice adito, il giudice del luogo in cui l'informazione messa in rete sia accessibile o lo sia stata<sup>55</sup>. La previsione della possibile operatività del *forum actoris*, che costituisce la significativa novità della sentenza *eDate*, corrisponde, secondo la Corte, al duplice obiettivo della buona amministrazione della giustizia e della prevedibilità, per l'attore, del giudice accessibile e, per il convenuto, del giudice dinanzi al quale può essere citato in giudizio<sup>56</sup>.

Pare opportuno sottolineare che tale disciplina è suscettibile di essere applicata entro l'ordinamento italiano a prescindere dal domicilio del convenuto, in base a quanto prevede l'art. 3, comma 2, l. n. 218/1995, con la conseguente ampia

---

<sup>50</sup> Corte di Giustizia CE, 7 marzo 1995, in causa C-68/93, *Shevill e a.*, cit., par. 23.

<sup>51</sup> Corte di Giustizia CE, 7 marzo 1995, in causa C-68/93, *Shevill e a.*, cit., par. 24.

<sup>52</sup> Corte di Giustizia CE, 7 marzo 1995, in causa C-68/93, *Shevill e a.*, cit., par. 29-30.

<sup>53</sup> Corte di giustizia UE, 25 ottobre 2011, in cause riunite C-509/09 e C-161/10, *E Date Advertising*, cit., par. 45-48.

<sup>54</sup> Corte di giustizia UE, 25 ottobre 2011, in cause riunite C-509/09 e C-161/10, *E Date Advertising*, cit., par. 48.

<sup>55</sup> Corte di giustizia UE, 25 ottobre 2011, in cause riunite C-509/09 e C-161/10, *E Date Advertising*, cit., par. 51.

<sup>56</sup> Corte di giustizia UE, 25 ottobre 2011, in cause riunite C-509/09 e C-161/10, *E Date Advertising*, cit., par. 50.

estensione del *forum actoris*. In altri Paesi, entro i quali non si è prevista l'estensione dell'operatività dei criteri del Regolamento Bruxelles I *bis* (come già di quelli della Convenzione di Bruxelles e del Regolamento Bruxelles I), per le ipotesi di violazioni dei diritti della personalità tramite *internet*, non si segue l'ampliamento operato dalla giurisprudenza di Lussemburgo, ma, ad es., si prevede che la giurisdizione dei tribunali nazionali si fondi su operazioni di *target marketing*, o di focalizzazione delle informazioni verso quel paese – come ad es. in Francia (art. 46 c.p.c.).

C'è tuttavia il rischio che l'azione volta a chiedere la rimozione dei contenuti lesivi immessi in *internet* si debba radicare solo dinanzi al foro in cui ha sede il convenuto<sup>57</sup>, e che secondo le indicazioni della Corte di Lussemburgo questa competenza attragga anche quella al risarcimento del danno – il fondamento della giurisdizione nel paese in cui la vittima di una lesione dei diritti della personalità deve cedere il passo alla giurisdizione fondata sulla richiesta di rimozione dei contenuti lesivi da un sito, con la conseguenza che la tutela della vittima non sia pienamente attuata in quanto radicata sempre e comunque dinanzi ai giudici del domicilio di chi gestisce le informazioni *online*.

Appare dunque evidente che, nonostante le indicazioni di molti Avvocati Generali<sup>58</sup> di semplificare la definizione della giurisdizione in caso di violazioni dei diritti della personalità tramite *internet*, la Corte di giustizia abbia ribadito l'approccio di definizione della giurisdizione "a mosaico", rendendo incerta e imprevedibile la soluzione dei casi. Si fa strada tuttavia, in dottrina, l'orientamento volto a delineare il c.d. approccio olistico, che privilegia il foro individuato dalla residenza della vittima<sup>59</sup>, nei casi in cui però vi sia un nesso con la violazione dei diritti della personalità della stessa.

Nelle ipotesi in cui i comportamenti lesivi dei diritti della personalità siano penalmente sanzionati entro gli ordinamenti nazionali<sup>60</sup>, l'art. 7, par. 3, del Regolamento Bruxelles I *bis* prevede che l'azione di risarcimento danni o di restituzione nascente da illecito penale sia sottoposta all'autorità giurisdizionale presso la quale è esercitata l'azione penale, se può conoscere dell'azione civile in base alla propria legge. Non sono molti, tuttavia, gli ordinamenti che sanzionano tutte le ipotesi di violazioni *online* dei diritti della personalità con una previsione criminosa *ad hoc*, come confermato dalla circostanza che la Direttiva recentemente adottata per

---

<sup>57</sup> Corte di giustizia UE, 17 ottobre 2017, C-194/16, *Bolagsupplysningen*, cit., par. 47.

<sup>58</sup> Conclusioni dell'Avv. Generale Villalón del 29 marzo 2011, nel caso *e Date*, ECLI: ECLI:EU: C:2011:192 e Conclusioni dell'Avv. Generale Bobek del 13 luglio 2017 nel caso *Bolagsupplysningen*, ECLI:EU:C:2017:554.

<sup>59</sup> A. DAVI, *Localisation du dommage d'origine delictuelle*, in *Riv. dir. int.*, 2022, p. 700 ss.

<sup>60</sup> Sul punto e sulla diffinitività degli ordinamenti nazionali in materia, attesa anche la molteplicità delle condotte riconducibili alla cyberviolenza, si v. in generale M.D. GOODMAN, S. BRENNER, *The Emerging Consensus on Criminal Conduct in Cyberspace*, in *Oxford International Journal of Law and Information Technology*, 2002, n. 2, p. 3.

contrastare la violenza nei confronti delle donne<sup>61</sup>, delinea – ai Consideranda – le motivazioni per le quali si rende necessario adottare norme minime in una materia frequentemente trascurata dagli Stati. Si pensi ad es. al caso del crimine di *revenge porn*, che in molti Paesi europei non ha una specifica previsione normativa volta a sanzionarne penalmente la condotta (eccetto Italia, Slovenia, Spagna), ma rientra nella più generale violazione del diritto alla privacy<sup>62</sup>.

In materia di responsabilità non contrattuale, originata da fattispecie collegate allo spazio virtuale, mette conto rilevare la giurisprudenza relativa ai casi in cui la stessa sia connessa a violazioni di marchi e istituti a tutela del diritto d'autore, prevalendo, in tale caso, il carattere territoriale di tali diritti, sui profili virtuali della lesione degli stessi.

La Corte di giustizia si è pronunciata nel caso *Wintersteiger*<sup>63</sup>, relativo alla violazione, da parte di una società tedesca (produttrice di accessori per lo sci commercializzati dalla società austriaca *Wintersteiger*), di un marchio austriaco soggetto a registrazione (per prodotti dello sci) in Austria, commessa mediante un'inserzione commerciale pubblicata su un motore di ricerca operante a livello globale, ma strutturato attraverso siti, con nomi di dominio di primo livello<sup>64</sup>, distinti per ciascun paese. La Corte ha affermato la non applicabilità del foro del centro di interessi, elaborato in materia di violazione dei diritti della personalità, ai diritti di proprietà intellettuale, in ragione della natura necessariamente territoriale di questi ultimi. Tale natura infatti, impone la necessaria localizzazione dell'evento dannoso nel territorio dello Stato che ha conferito il diritto e lo protegge<sup>65</sup>. Nel caso di specie, ai fini della prevedibilità e della corretta amministrazione della giustizia, la competenza viene riconosciuta, sulla base della concretizzazione del danno, ai giudici dello Stato membro in cui il diritto in causa è tutelato, ai quali è conferita anche la piena cognizione relativamente ai danni cagionati. La competenza dei giudici austriaci si

---

<sup>61</sup> Direttiva (UE) 2024/1385 del Parlamento europeo e del Consiglio del 14 maggio 2024 sulla lotta alla violenza contro le donne e alla violenza domestica, in *GUUE*, del 24 maggio 2024, L 1/36. Sul punto si v. A. DI STASI, R. ESPINOSA CALABUIG (a cura di), *Cyberviolenza di genere e nuove "frontiere" normative e giurisprudenziali: la direttiva UE 2024/1385, Ciberviolencia de género y nuevas "fronteras" normativas y jurisprudenciales: la directiva UE 2024/1385*, Napoli, 2025.

<sup>62</sup> M. ŠEPEC, *Revenge Pornography or Non-Consensual Dissemination of Sexually Explicit Material as a Sexual Offence or as a Privacy Violation Offence*, in *International Journal of Cyber Criminology*, 2019, p. 418 ss.

<sup>63</sup> Corte di giustizia dell'Unione europea, 19 aprile 2012, C-523/10, *Wintersteiger AG c. Products 4U Sondermaschinenbau GmbH*, ECLI:EU:C:2012:220.

<sup>64</sup> Per nome di dominio di primo livello si fa riferimento alla parte finale di un indirizzo *internet*, la quale serve a identificare i siti web in base a determinate categorie o aree geografiche. Ad es., per l'Italia, il dominio di primo livello è identificato nel dominio nazionale ".it"; per la Spagna si utilizza ".es"; per la Germania ".de".

<sup>65</sup> N. BOSCHIERO, *Il principio di territorialità in materia di proprietà intellettuale: conflitti di legge e giurisdizione*, in *Annali italiani del diritto d'autore, della cultura e dello spettacolo (AIDA)*, 2007, p. 81.

riconosce quindi in quanto autorità dello Stato membro di registrazione, indipendentemente dal fatto che la pubblicazione dell'annuncio lesivo da parte della convenuta fosse rivolta esclusivamente al mercato tedesco.

La Corte di giustizia ha confermato l'indirizzo espresso nella sentenza *Wintersteiger*, in due sentenze (*Pinckney*<sup>66</sup> e *Hejduk*<sup>67</sup>), nell'ambito delle quali è stata affrontata - dinanzi al giudice del luogo di concretizzazione del danno - la questione del *locus damni* in relazione a violazioni *online* del diritto d'autore, a causa della riproduzione e commercializzazione delle opere intellettuali di alcuni autori mediante i siti *web* di alcune società. In entrambi i casi, la Corte ha confermato la giurisdizione dei giudici del rinvio pregiudiziale, in forza della direttiva CE 29/2001, secondo la quale i diritti patrimoniali di un autore devono essere automaticamente protetti in tutti gli Stati membri, non richiedendosi che l'attività dannosa sia "diretta verso" lo Stato membro del giudice adito, superando così le argomentazioni delle società convenute concernenti la circostanza che i propri siti *web* non erano destinati al pubblico di quegli Stati membri.

Nella giurisprudenza appena considerata, il mero accesso al sito *web* tramite il quale sono stati diffusi i contenuti protetti, è stato dunque ritenuto elemento sufficiente ai fini della concretizzazione del danno in uno Stato membro.

## 5. Legge applicabile

L'individuazione della legge applicabile in materia di rapporti internazionali privatistici fondati sullo sviluppo delle tecnologie evidenzia notevoli complessità, determinate dalla difficile qualificazione delle fattispecie da disciplinare, quale operazione necessaria a tal fine<sup>68</sup>.

---

<sup>66</sup> Corte di giustizia dell'Unione europea, 3 ottobre 2013, C-170/12, *Peter Pinckney c. KDG Mediatech AG*, ECLI:EU:C:2013:635.

<sup>67</sup> Corte di giustizia dell'Unione europea, 22 gennaio 2015, C-441/13, *Pez Hejduk c. EnergieAgentur.NRW GmbH*, ECLI:EU:C:2015:28.

<sup>68</sup> Sulla qualificazione nel diritto internazionale privato, si veda in generale E. BARTIN, *Principes de droit international privé*, Paris, 1930, vol. I, p. 221; F. KAHN, *Gesetzeskollisionen*, cit., pp. 1-123; F. RIGAUX, *La Théorie des Qualifications en droit international privé*, Paris, 1956, p. 17 ss.; R. AGO, *Teoria del diritto internazionale privato*, Padova, 1934, p. 138 ss.; W. WENGLER, *Die Qualifikation der materiellen Rechtssätze im internationalen Privatrecht*, in *Festschrift für Wolff*, Tübingen, 1952, pp. 337-374; ID., *Réflexions sur la technique des qualifications en droit international privé*, in *Revue critique de droit international privé*, 1954, pp. 661-691; A.N. MAKAROV, *Theorie und Praxis der Qualifikation*, in *Vom deutschen zum europäischen Recht*, *Festschrift für Dölle*, Tübingen, 1963, vol. II, p. 148 ss.; Ph. FRANCESCAKIS, *Conflits de Lois (principes généraux)*, in *Répertoire de droit international*, Dalloz, Paris, 1968, vol. I, pp. 470-497, p. 490; H. WEBER, *Die Theorie der Qualifikation*, Tübingen, 1986, p. 15 ss.; M. LEHMANN, *Les Qualifications*, in *Juris - Classeur de droit international*,

È d'altra parte noto che gli istituti richiamati dalle norme di conflitto dei regolamenti UE di diritto internazionale privato vadano interpretati alla luce del diritto sostanziale dell'Unione<sup>69</sup>, o delle indicazioni della Corte di giustizia dell'Unione europea nella definizione delle categorie giuridiche richiamate dai regolamenti internazionaliprivatistici<sup>70</sup>.

È dunque possibile affermare che, ove siano adottati atti dell'Unione europea in tema di fattispecie connesse all'esplicarsi della sovranità digitale, il riferimento alle nozioni dagli stessi previste risolva i problemi di qualificazione.

Si pensi ad es. alla Direttiva 2002/47 sui contratti di garanzia finanziaria<sup>71</sup>, secondo la quale le questioni derivanti da una garanzia su strumenti finanziari in forma scritturale vengono regolate dalla legge dello Stato in cui è situato il conto di pertinenza. Tra le "questioni", cui si rinvia al paragrafo 1, ricorrono «la natura giuridica e gli effetti patrimoniali della garanzia su strumenti finanziari in forma scritturale», i «requisiti di perfezionamento di un contratto di garanzia finanziaria concernente la garanzia su strumenti finanziari in forma scritturale (...)», «se un diritto di proprietà o altro diritto concorrente di una persona a siffatta garanzia su strumenti finanziari in forma scritturale prevalga o sia subordinato a un diritto di proprietà o altro diritto concorrente o se abbia avuto luogo un acquisto in buona fede», e infine «le modalità con le quali la garanzia su strumenti finanziari in forma scritturale deve essere realizzata dopo un evento determinante la sua escussione» (art. 9). Ciò, analogamente a quanto previsto dalla Direttiva 98/26/CE concernente il carattere definitivo del regolamento nei sistemi di pagamento e nei sistemi di regolamento titoli<sup>72</sup>, per cui per i diritti reali di garanzia costituiti su strumenti finanziari e legalmente registrati in un libro contabile, conto o sistema di deposito accentrato situato in uno Stato membro, «la determinazione dei diritti di tali enti

---

Paris, 1988, fasc. 531, pp. 1-34; C. BERNASCONI, *Der Qualifikationsprozess im Internationalen Privatrecht*, Zürich, 1997, p. 84 ss.; K. LIPSTEIN, *Characterization*, in *International Encyclopedia of Comparative Law*, III, *Private International Law*, 5, 1999, pp. 3-35, p. 22.

<sup>69</sup> M. AUDIT, *L'interprétation autonome du droit international privé communautaire*, in *Journal du droit international*, 2004, p. 789 ss.; R. BARATTA, *The Process of Characterization in the EC Conflict of Laws: Suggesting a Flexible Approach*, in *Yearbook of Private International Law*, 2004, p. 171 ss.; S. BARIATTI, *Qualificazione e interpretazione nel diritto internazionale privato comunitario: prime riflessioni*, in *Riv.dir.int.priv.proc.*, 2006, p. 361 ss.

<sup>70</sup> F. SALERNO, *L'impatto della procedura di interpretazione pregiudiziale sul diritto internazionale privato nazionale*, in *Riv. dir. int. priv. proc.*, 2023, p. 5 ss.

<sup>71</sup> Direttiva 2002/47/CE del Parlamento europeo e del Consiglio del 6 giugno 2002 relativa ai contratti di garanzia finanziaria, in *GUUE* L 168 del 27 giugno 2002.

<sup>72</sup> Direttiva 98/26/CE del Parlamento europeo e del Consiglio del 19 maggio 1998 concernente il carattere definitivo del regolamento nei sistemi di pagamento e nei sistemi di regolamento titoli, in *GUUE*, L 166 dell'11 giugno 1998, modificata dal Regolamento (UE) 2024/886 del Parlamento europeo e del Consiglio del 13 marzo 2024, in *GUUE*, L 886 del 19 marzo 2024.

come detentori dei titoli costituiti in garanzia è disciplinata dalla legge di detto Stato membro».

La definizione dell'ambito d'applicazione della c.d. *lex conto sitae*<sup>73</sup> non risolve, tuttavia, il problema di qualificazione delle nuove forme di pagamento, quali ad es. le criptovalute, cui si esclude possano applicarsi gli atti normativi ora in esame<sup>74</sup>.

Pertanto il problema di qualificazione si ripresenta nel momento in cui si presentino dei casi in cui tali istituti divengano oggetto di controversie internazionali-privatistiche.

Come qualificare ad es. la proprietà delle criptovalute, nel caso in cui un investitore abbia subito un furto in seguito ad un'operazione di hackeraggio?

Stabilire se le criptovalute possano costituire oggetto di proprietà è essenziale, per comprendere se esse possano essere oggetto di misure cautelari ed esecutive, nonché di istituti come la custodia, la garanzia, la successione, l'insolvenza, ecc. Una categoria specifica di beni immateriali in cui le criptovalute potrebbero essere fatte rientrare è quella degli strumenti finanziari, per cui sarà opportuno valutare l'applicazione alle criptovalute delle regole internazionali-privatistiche concernenti tali istituti.

Tale aspetto va tuttavia scisso dalla qualificazione del rapporto contrattuale cui le criptovalute ineriscono e da eventuali profili di responsabilità non contrattuale.

Tornando al caso, appena prospettato, di hackeraggio, è chiaro che nei rapporti tra risparmiatore e piattaforma che ospita l'investimento varrà la legge applicabile al contratto di utilizzazione della piattaforma. Nell'ipotesi in cui il risparmiatore intenda agire civilmente nei confronti dell'*hacker* per ottenere un risarcimento dei danni da responsabilità non contrattuale, occorrerà seguire le norme del Regolamento Roma II, prospettandosi così l'operatività della *lex damni*, o della *lex loci delicti*, o della legge che presenta il collegamento più stretto.

Quest'ultimo aspetto evidenzia particolari criticità, posto che per concretizzare tale criterio occorrerebbe localizzare vari aspetti: l'hackeraggio – operazione complessa e spesso impossibile, soprattutto perché – come noto – gli *hackers* lavorano spesso da più luoghi (virtuali) diversi, e magari entro uno Stato – ammesso che si riesca a localizzare – in cui l'hackeraggio non è considerato illegale; la localizzazione degli investitori – difficile poiché gli stessi hanno spesso un portafogli virtuale –

---

<sup>73</sup> F.C. VILLATA, *Gli strumenti finanziari nel diritto internazionale privato*, Padova, 2008, p. 33; M. LEHMANN, *Financial Instruments*, in J. BASEDOW, G. RÜHL, F. FERRARI, P. DE MIGUEL ASENSIO (eds.), *Encyclopedia of Private International Law*, Edward Elgar Publishing, Cheltenham, 2017, p. 739 ss.; A. RUZIK, *Settlement Finality Directive (SFD)*, in M. LEHMANN, C. KUMPAN (eds.), *European Financial Services Law*, Baden-Baden, 2019, pp. 1703-1704.

<sup>74</sup> M. LEHMANN, *How to Determine the Law Applicable to Crypto Assets?*, The EAPIL Blog, 2 aprile 2021, disponibile all'indirizzo: <https://eapil.org/2021/04/02/how-to-determine-the-law-applicable-to-crypto-assets>.

*wallet* – che si trova nel computer, ma anche nel *cloud*, oppure su un *device* separato. Si può allora immaginare di utilizzare la residenza dell'investitore per regolare il risarcimento dei danni in caso di furto di criptovalute? È probabile che si debba sciogliere in maniera affermativa tale quesito, ma si tratta di un criterio che non dà conto del fatto che l'investitore può collegarsi alle piattaforme per eseguire gli investimenti non necessariamente dal luogo della propria residenza, ma da un luogo casuale.

Più in generale, si tratta anche in questo contesto, come già si è visto in tema di criteri di giurisdizione<sup>75</sup>, di adattare i criteri di collegamento vigenti alle tipologie di istituti c.d. digitali.

Si pensi ad es. al criterio di collegamento dell'*electio iuris*, pietra angolare del Regolamento Roma I. Difficilmente tale criterio sarà applicabile – secondo quanto prevede l'art. 3 del Regolamento Roma I – ai contratti conclusi tramite *blockchains* che richiedono una cooperazione su molteplici livelli e in molti Stati differenti ove si localizzano tutte le parti coinvolte nell'operazione finanziaria<sup>76</sup>. L'utilizzo della tecnologia per la conclusione del contratto non esclude la qualificazione contrattuale e la riconducibilità degli *smart contracts* alla disciplina del regolamento Roma I<sup>77</sup>, ma solo la difficoltà di ricostruire l'operatività di criteri di collegamento codificati per regolare rapporti tra persone (fisiche e giuridiche) – quale appunto la scelta di legge delle parti contrattuali – a fattispecie in cui manca l'azione umana. Gli *smart contracts* conclusi tramite *blockchain* utilizzano infatti reti di dati, che possono configurare sistemi di pagamento (PayPal), di prenotazioni, di prestito, ecc. Come si è detto, i diritti sui rapporti costituiti tramite *blockchain* sono inseriti in un *token*, uno strumento informatico ricognitivo di una posizione giuridica su di un bene o su un rapporto obbligatorio emesso dal soggetto passivo a fronte di un apporto avente valore economico e che consente al soggetto attivo di esercitare uno o più diritti nei confronti dell'emittente. Può rientrare in un *token* la proprietà di un bene, un diritto di credito, azioni, obbligazioni e altri strumenti finanziari; si distinguono generalmente i *payment token*, gli *utility token* e gli *investment token*<sup>78</sup>.

---

<sup>75</sup> Si v. sul punto *supra* par. 4, 4.1, 4.2.

<sup>76</sup> P. DE FILIPPI, A. WRIGHT, *Blockchain and the Law*, Cambridge, 2018, p. 21; Y. CHIU, *Regulating the Crypto Economy*, Oxford-New York, 2021, p. 220 ss.

<sup>77</sup> B. AUDIT, *Le droit international privé confronté à la blockchain*, in *Revue critique de droit international privé*, 2020, p. 685 ss.; G. RÜHL, *Smart (Legal) Contracts, or: Which (Contract) Law for Smart Contracts?*, in B. CAPPIELLO, G. CARULLO (eds.), *Blockchain, Law and Governance*, Cham, 2021, p. 165 ss.

<sup>78</sup> Su tale classificazione, si v. Autorità bancaria europea (ABE), *Report with advice for the European Commission on crypto-assets*, 9 gennaio 2019, p. 7 ss., Autorità europea degli strumenti finanziari e dei mercati (ESMA), *Advice on Initial Coin Offerings and Crypto-Assets*, ESMA50-157-1391, 9 gennaio 2019, p. 11.

I *payment token* rappresentano valori digitali che replicano la funzionalità della moneta come mezzo di scambio avente corso convenzionale all'interno di un mercato; gli *utility token* conferiscono al legittimato il diritto di usufruire di un servizio o di ricevere un bene che l'emittente gli deve trasferire tramite un *token* – possono anche qualificarsi come voucher, come espressamente previsto in una delle poche legislazioni nazionali a disciplinare la materia, ovvero la legge di San Marino del 2019<sup>79</sup>, ovvero come documenti di legittimazione nell'ordinamento italiano (art. 2002 c.c.). Gli *investment token* rappresentano partecipazioni sociali, obbligazioni e altri strumenti finanziari che conferiscono al legittimato diritti patrimoniali e/o amministrativi nei confronti della società emittente; funzionalmente potrebbero essere assimilati alle azioni, ma giuridicamente è escluso che possano essere ricondotti a tale categoria in forza dell'anonimato che caratterizza le *blockchain*. Nell'ordinamento italiano è complicato classificarli, attesa anche la tipicità legale dei titoli di credito al portatore (art. 2004 c.c.).

È inoltre difficile ipotizzare l'operatività dell'*optio iuris*, attesa la molteplicità dei soggetti coinvolti in tale ambito, nonostante questa sia, tra l'altro, la soluzione proposta dalla Convenzione dell'Aja del 5 luglio 2006, sulla legge applicabile a titoli finanziari detenuti presso un intermediario (banca, broker, custode), in vigore dal 2017 seppure per un numero limitatissimo di Stati (Svizzera, USA, Mauritius)<sup>80</sup>. È la prima Convenzione che si occupa di individuare la legge applicabile ai titoli finanziari dematerializzati e individua come criterio principale *l'electio iuris*, prevedendo – solo in assenza di scelta di legge – l'operatività della legge dello Stato in cui l'intermediario ha il conto finanziario. Rispetto alla disciplina da essa prevista, occorre inoltre rilevare che la regola applicabile in assenza di scelta di legge appare di difficile estensione ai contratti finanziari conclusi tramite *blockchain*, poiché – con riguardo a questi ultimi – manca l'intermediario che è la rete tecnologica, di difficile localizzazione anche per quanto riguarda la gestione del conto corrente. Un aspetto interessante che invece la Convenzione dell'Aja contempla è la disciplina dei diritti dei terzi in caso di insolvenza, e tale aspetto potrebbe estendersi ai casi dei contratti conclusi tramite *blockchain*.

Appare inoltre particolarmente complesso applicare i criteri di collegamento vigenti in materia di obbligazioni non contrattuali. Si pensi ad es. al caso concernente uno *smart contract* di prestito in cui chi presta i soldi ha la propria residenza in

---

<sup>79</sup> Decreto delegato 23 maggio 2019, n. 86 “Norme sulla tecnologia *blockchain* per le imprese”.

<sup>80</sup> Al riguardo, va rilevato l'ambiguo atteggiamento dell'Unione europea. Dopo un'iniziale apertura nei confronti della ratifica della convenzione dell'Aja del 2006 sulla legge applicabile ad alcuni diritti su strumenti finanziari detenuti presso un intermediario, la Commissione ha successivamente ritirato la proposta di decisione del Consiglio relativa alla firma; cfr. Proposta di decisione del Consiglio riguardante la firma della convenzione dell'Aja sulla legge applicabile ad alcuni diritti su strumenti finanziari detenuti presso un intermediario, COM(2003) 783 def., 15 dicembre 2003.

Italia e chi li riceve ha la residenza a Singapore. Le parti si accordano che il prestito debba essere rimborsato in criptovalute (eteri). Immaginiamo che per un errore del codice *blockchain* il pagamento del prestito sia effettuato al portafogli di persona diversa dal creditore. Per ottenerne la restituzione dell'indebitito, si potrà fare riferimento, quanto alla legge applicabile, all'art. 10 del Regolamento Roma II: legge scelta dalle parti del contratto, legge dello Stato di residenza di entrambi, legge dello Stato di residenza della vittima dell'ingiusto arricchimento. La peculiarità della fattispecie, realizzata in maniera virtuale tramite una serie di connessioni di rete, evidenzia la necessità di interpretare la norma ora in esame, preferendo la facilità di localizzazione offerta dai criteri di collegamento soggettivi.

Alla luce di tali difficoltà, parte della dottrina, considerando la natura del procedimento *blockchain* che si basa sulla fiducia reciproca negli algoritmi, evidenzia, anche in questo caso, la possibilità di superare le regole tradizionali del diritto internazionale privato per definire un'autonoma disciplina del procedimento *blockchain*, una c.d. *lex numerica*, o *lex cryptography*, e un corrispondente sistema autonomo di soluzione delle eventuali controversie, una *Computer Dispute Resolution*, svincolata dalla sovranità giurisdizionale degli Stati<sup>81</sup>.

Si tratterebbe di una soluzione coerente a presupposti e funzionamento del *blockchain*, ma difficile da attuare in quanto le transazioni tramite *blockchain* non sono necessariamente isolate da altri contesti giuridici transnazionali in cui la ricerca della legge applicabile rimane un aspetto fondamentale: si pensi ad es. ad un contratto di prestito tramite *blockchain* entro il quale il rimborso viene attivato autonomamente alla scadenza prevista dalle parti, ma chi ha assunto il prestito è in una situazione di fallimento; la disciplina del prestito andrebbe dunque coordinata con quella del fallimento trattandosi di un credito che va ad inserirsi nella procedura fallimentare.

L'analisi di quest'ultimo caso evidenzia un altro problema: il distacco del mondo virtuale da quello reale può avere effetti dirompenti, visto che le circostanze stabilite nel procedimento *blockchain* non possono essere modificate in seguito ad avvenimenti della vita reale e ciò potrebbe anche determinare il fallimento di un contraente.

Appare dunque evidente che solo il diritto internazionale privato ha gli strumenti per collegare il mondo virtuale al reale, per consentire ad es. tramite la proroga di giurisdizione e la clausola di scelta di legge, seppure nelle difficoltà applicative poste dagli istituti in esame, che le parti di un contratto concluso tramite *blockchain* abbiano adeguate garanzie in merito al foro competente e alla legge applicabile ai loro rapporti.

La necessità di operare un coordinamento tra le diverse fonti del diritto internazionale

---

<sup>81</sup> A. WRIGHT, P. DE FILIPPI, *Decentralized Blockchain Technology and the Rise of Lex Cryptographia*, cit.

privato è ulteriormente confermata dall'interrelazione tra il Regolamento (UE) 2023/1114 relativo ai mercati delle cripto-attività (di seguito Regolamento MiCAR)<sup>82</sup>, e il Regolamento Roma I in materia di tutela dei consumatori<sup>83</sup>.

Come già osservato in tema di giurisdizione rispetto all'art. 17 del Regolamento Bruxelles I *bis*<sup>84</sup>, l'acquisto di criptovalute su piattaforme di investimento può rientrare nella nozione dell'art. 6 del Regolamento Roma I, ovvero nei contratti formati tra un soggetto che esercita un'attività commerciale o professionale, nell'espletamento di tali funzioni e una persona fisica che agisce al di fuori della sua attività economica o professionale. La giurisprudenza di Lussemburgo è intervenuta a chiarire vari aspetti di questa disposizione formulata con una formulazione in negativo, tra cui ad es. il limite alla flessibilità della nozione in esame, nell'ipotesi in cui la parte contrattuale che opera nello svolgimento di un'attività economica sia ragionevolmente inconsapevole dello *status* di consumatore dell'altra, poiché le circostanze impediscono di accertare che questa agisca in qualità di privato<sup>85</sup>. L'utilizzo di pseudonimi da parte dei partecipanti ai circuiti di acquisto delle criptovalute potrebbe precludere la configurabilità degli accordi venutisi a creare tra utenti come contratti del consumatore, a meno che le parti non siano legate da un rapporto preesistente.

Più complessa è la considerazione delle relazioni instaurate tra utenti e gestori di sistemi di criptovalute privati, istituti finanziari tradizionali che propongono servizi di investimento in materia di criptovalute o piattaforme di investimento *online*, che ampliano la propria offerta alle criptovalute. In questi casi, infatti, la fattispecie descritta dall'art. 17 del Regolamento Bruxelles I *bis*, e dall'art. 6 del Regolamento Roma I viene integrata nella misura in cui ricorra un'attività commerciale da un lato del rapporto, e un privato la cui identità è nota alla piattaforma, al consulente o all'amministratore del circuito privato e *permissioned*, dall'altro<sup>86</sup>. Anche l'esenzione prevista all'art. 6(4)(d) del Regolamento Roma I per i «diritti e obblighi che costituiscono uno strumento finanziario, e dei diritti e obblighi costitutivi delle clausole e condizioni che disciplinano l'emissione o l'offerta al pubblico e le offerte pubbliche di acquisizione di valori mobiliari, e alla sottoscrizione e al riacquisto di

---

<sup>82</sup> Regolamento (UE) 2023/1114 del Parlamento europeo e del Consiglio, del 31 maggio 2023, relativo ai mercati delle cripto-attività e che modifica i Regolamenti (UE) n. 1093/2010 e (UE) n. 1095/2010 e le Direttive 2013/36/UE e (UE) 2019/1937, in *GUUE* L 150 del 9 giugno 2023. Si v. sul punto F. VILLATA, *Il regolamento UE (2023)/1114 relativo ai mercati delle cripto-attività: prime note nella prospettiva del diritto internazionale privato*, in *Riv. dir. int. priv. proc.*, 2023, p. 754 ss.

<sup>83</sup> B. AUDIT, *Le droit international privé confronté à la blockchain*, cit., p. 686.

<sup>84</sup> Si v. sul punto *supra* par. 4.1.

<sup>85</sup> CGUE, sentenza del 20 gennaio 2005, causa C-464/01, *Johann Gruber c. Bay Wa AG*, par. 51, ECLI: ECLI:EU:C:2005:32.

<sup>86</sup> B. RIPLEY, *Cryptocurrency Transfers in Distributed Ledger Technology-Based Systems and their Characterisation in Conflict of Laws*, in J. BORG-BARTHET, K. TRIMMINGS, B. RIPLEY, P. ŽIVKOVIC (eds.), *From Theory to Practice in Private International Law*, Oxford, 2024, p. 120.

quote di organismi di investimento collettivo, nella misura in cui tali attività non costituiscono prestazione di un servizio finanziario» non pare interessare le relazioni contrattuali in oggetto, data la difficoltà, già evidenziata, di ascrivere le criptovalute agli strumenti finanziari. Peraltro, il considerando n. 29 del regolamento MiCAR mantiene ferma l'applicabilità degli atti UE contenenti regimi di favore per i consumatori alle offerte al pubblico di cripto-attività, quando oggetto di controversia è la relazione tra imprese e consumatori. Questa indicazione non fa che confermare l'applicabilità della normativa posta dal regolamento Roma I a protezione del consumatore ai rapporti in esame<sup>87</sup>.

## 6. Osservazioni conclusive

Il diritto internazionale privato possiede strumenti che consentono di avvicinare ad un ordinamento fattispecie transnazionali che non hanno una connessione territoriale, in quanto virtualmente collegate allo spazio di *internet*. Si tratta, tuttavia, di ripensare alle regole tradizionalmente volte a risolvere i conflitti di leggi e di giurisdizioni, al fine di consentire una migliore efficacia delle stesse a supporto della tutela dei diritti fondamentali.

In primo luogo viene in rilievo il principio di territorialità, come strumento utilizzato anche dal diritto internazionale privato al fine di assicurare certezza e prevedibilità alla soluzione delle controversie tra privati, sulla base della connessione territoriale delle stesse con la giurisdizione di un determinato paese o la legge applicabile. In contesti quali quelli inerenti alla sovranità tecnologica, che si esplica via *internet*, la connessione territoriale non sembra più essere lo strumento idoneo a definire competenza giurisdizionale e legge applicabile<sup>88</sup>.

Emerge allora la necessità di esplorare, da un lato, l'operatività di altri criteri di collegamento, non basati sul principio di territorialità ma su altri principi, come ad es. la cittadinanza, il domicilio, la residenza delle parti, con tutte le criticità che tali criteri portano con sé, in seguito all'evoluzione tecnologica. I collegamenti soggettivi svelano ad es. alcune complessità nella disciplina dei rapporti fondati su *blockchain* in cui non vi è intermediazione umana, le parti concludono un contratto senza conoscersi e senza coinvolgimento di un intermediario; difficile pertanto definire il domicilio del convenuto o la residenza abituale del debitore della prestazione caratteristica.

Dall'altro lato, la crisi del principio di territorialità evidenzia il ruolo strategico della volontà delle parti, sia ai fini dell'individuazione del giudice competente sia in ordine alla definizione della legge applicabile<sup>89</sup>.

---

<sup>87</sup> F. VILLATA, *Il regolamento UE (2023)/114*, cit., p. 752.

<sup>88</sup> A. MILLS, *The Law Applicable to Cross-border Defamation*, cit.

<sup>89</sup> F.K. JUENGER, *Choice of Law and Multistate Justice*, Dordrecht, 1993.

Resta da chiarire come tale criterio possa declinarsi nei rapporti in cui le parti negoziano tramite reti tecnologiche e dunque in che modo possa dirsi recepita la volontà effettiva delle stesse.

Si tratta di approcci diversi alla soluzione dei problemi tradizionali del diritto internazionale privato, che però evidenziano un differente modo di considerare le relazioni tra Stati, a partire dalla necessità di affermare la sovranità tecnologica o digitale in assenza di uno spazio territoriale. In considerazione del ruolo saliente dei diritti fondamentali, appare tuttavia chiaro che tali regole vanno ripensate al fine di assicurare una più efficace tutela di tale obiettivo, non diversamente realizzabile tramite altre prospettazioni, quale ad es. la generale operatività della *lex fori*<sup>90</sup>.

---

<sup>90</sup> F. GUILLAUME, *Aspects of private international law related to blockchain transactions*, in D. KRAUS, T. OBRIST, O. HARI (eds.), *Blockchains, Smart Contracts, Decentralised Autonomous Organisation and the Law*, Elgar, 2019, p. 49 ss.

Finito di stampare nel mese di febbraio 2026  
nella LegoDigit s.r.l. – Via Galileo Galilei 15/1  
38015 Lavis (TN)