MARIO CARTA

DIRITTO ALLA VITA PRIVATA ED INTERNET NELL'ESPERIENZA GIURIDICA EUROPEA ED INTERNAZIONALE

SOMMARIO: 1. Strumenti internazionali di protezione dei diritti umani sul *web* e ruolo dell'analogia. — 2. Diritto alla vita privata e protezione dei dati personali *on line* nel sistema CEDU. — 3. Ruolo e responsabilità degli intermediari nella protezione dei dati personali in Europa. — 4. Prospettive di riforma della protezione dei dati personali nella U.E. — 5. Conclusioni.

1. Strumenti internazionali di protezione dei diritti umani sul *web* e ruolo dell'analogia.

Il presente lavoro si propone di affrontare ed approfondire alcuni delle sfide, ma anche delle opportunità, che l'orizzonte giuridico di Internet, come è stato definito ormai qualche anno fa con una espressione che conserva ancora oggi tutta la sua attualità [1], pone alla sovranità territoriale così come la abbiamo conosciuta e la conosciamo, ma soprattutto al sistema dei diritti umani [2] che quella nozione di sovranità ha in qualche modo contribuito a garantire ed assicurare. Sfide in quanto l'uso sempre più pervasivo delle nuove tecnologie in Rete ha accresciuto in

* Il presente scritto è stato preventivamente sottoposto a refcraggio anonimo affidato a un componente il Comitato Scientifico dei Referenti della Rivista secondo le correnti prassi nella comunità dei giuristi.

[1] In tal senso vedi V. Frosini, *L'orizzonte giuridico dell'Internet*, in *Il diritto dell'informazione e dell'informatica*, 2000, 271 e ss.

[2] Per il rapporto tra diritti umani, sovranità territoriale ed Internet nella dottrina internazionalistica vedi tra gli altri, a cura di K. Benyekhlef e P. Trudel, *État de droit et virtualité*, Montréal, 2009 in particolare K. Benyekhlef, *Une réformation de l'État-nation: vers une souveraineté virtuelle?*, pp. 123-156; D. Alland, *Les représentations de l'espace en droit international public*, in *Archives de philosophie du droit*, 1986, pp. 163-178; H. Ruiz-Fabri, in *Immatériel, territorialité, et l'État*, in *Archives de philosophie du droit*, 1999, pp. 187-212; P. Jacob, *La Gouvernance de l'Internet du point de vue du droit international public*, in *Annuaire français de droit international*, 2011, pp. 543-563; R. Uerpmann-Wittack, *Principles of International Internet Law*, in *German Law Journal*, 2010, pp. 1245-1263; Y. Benkler, *Internet Regulation: A Case Study on the Problem of Unilateralism*, in *European Journal of International Law*, 2010, pp. 171-185; J. Goldsmith, *Unilateral Regulation of the Internet: A Modeste Defense*, in *European Journal of Inter-*

maniera significativa le forme e le modalità attraverso le quali i diritti umani possono essere messi a rischio, in particolare il diritto alla vita privata nella sua manifestazione oggi più evidente e cioè la protezione dei dati di carattere personali immessi in Rete da ognuno di noi, e, dall'altra, opportunità in quanto quello che è ormai noto come il "più grande spazio pubblico che l'umanità abbia conosciuto" [3] consente una tale libertà di espressione, comunicazione ed informazione in favore e da parte degli utenti della Rete [4], da renderlo uno dei più efficaci strumenti di partecipazione democratica e di promozione degli stessi diritti umani. Alcune delle caratteristiche che delineano la specificità della tutela dei diritti umani in relazione al *web* sono state messe in luce nei numerosi studi dedicati, in una prospettiva prevalentemente nazionale, alla qualificazione ed esistenza del diritto di accesso ad Internet [5], tema che quindi non verrà toccato in questa sede anche in quanto gli elementi in favore dell'esistenza di una norma a carattere consuetudinario non sembrano essere così solidi [6]; l'attenzione sarà rivolta invece alle implicazioni che la nuova dimensione spaziale e temporale connaturata alla Rete produce sul sistema dei diritti umani ed al loro esercizio nella c.d. società digitale, ed in particolare al diritto al rispetto della vita privata,

national Law, 2010, pp. 135-148; M.C. KETTEMANN, *The Future of Individuals in International Law, Lessons from International Internet Law*, L'Aja, 2013; J. KULESZA, *International Internet Law*, Abingdon, 2012. Per la dottrina internazionalistica italiana, non particolarmente ricca per la verità sul punto, vedi di recente M. RUOTOLO, *Internet-ional Law, Profili di diritto internazionale pubblico della Rete*, Bari, 2012 in particolare pp. 113-125, e A. VALVO, *Diritti umani e realtà virtuale, Normativa europea ed internazionale*, Roma 2013.

[3] Per questa espressione S. RODOTÀ, *Il diritto ad avere diritti*, Bari, 2012, p. 379.

[4] Sul progressivo affievolimento della distinzione tra libertà di comunicazione e di manifestazione del pensiero legata al fatto che oggi tutti possono essere al tempo stesso comunicatori e diffusori vedi V. ZENO-ZENCOVICH: "Nell'attuale realtà uno stesso mezzo-la rete- rende tutti coloro che vi hanno accesso in soggetti che possono scegliere se utilizzarlo per comunicazioni interpersonali o per diffondere il proprio pensiero. Ed eliminare l'utente finale", in *Perché occorre rifondare il significato della libertà di manifestazione del pensiero*, in *Percorsi costituzionali*, n. 1, 2010, pp. 69-75, in particolare p. 73. Per il rapporto tra diritto alla riservatezza e diritto alla informazione nell'ordinamento italiano vedi P. CARETTI, A. CARDONE, *Diritto alla riservatezza e diritto all'informazione: premesse normative e sviluppi giurisprudenziali*, in *Diritti umani e diritto internazionale*, 2010, pp. 87-103.

[5] Per il diritto di accesso ad Internet considerato quale diritto sociale costituzionale, o meglio, quale pretesa soggettiva a prestazioni pubbliche vedi T. FROSINI, *Il diritto costituzionale di accesso ad Internet*, in *Rivista Associazione italiana dei costituzionalisti (AIC)*, 1/2011, p. 8. Nel senso invece del diritto di accesso quale precondizione per l'esercizio in Rete di alcuni diritti costituzionali (in particolare quelli di cui agli artt. 15 e 21 della Costituzione) ai quali sarebbe legato da un nesso di strumentalità, vedi V. ZENO-ZENCOVICH, *L'accesso alla rete come diritto fondamentale*, Relazione al convegno "Il diritto dell'informazione tra regole antiche e nuovi media", Secondo seminario di studi in ricordo di Corso Bovio, Milano 20 maggio 2010. Da ultimo sul punto M. BETZU, *Regolare Internet: le libertà di informazione e comunicazione nell'era digitale*, Torino 2012, in particolare pp. 86-93.

[6] Si attende a breve l'esito del ricorso presentato a Strasburgo da un cittadino lituano detenuto che si è visto negare, in carcere, l'accesso ad Internet per potersi iscrivere all'università: Jankovskis c. Lituania, ricorso n. 21575/08 già comunicato nel settembre del 2010 al governo interessato.

intesa quale protezione dei dati personali, che appare oggi uno dei diritti più seriamente messi in discussione dal *web*. Per descrivere tali caratteristiche sono state coniate espressioni suggestive, ed anche efficaci quali "Dio perdona e dimentica, la Rete mai" che allude al tema della permanenza nella Rete in modo pressoché senza limiti di tempo dei dati e delle tracce che ci riguardano e che richiama il diritto all'oblio quale probabilmente ultima frontiera della tutela dei dati personali *on line* [7]; o all'espressione"ogni cosa, in ogni luogo, in ogni momento" che accanto alla natura istantanea ed all'immediatezza delle informazioni che circolano sul *web*, vuole sintetizzare il diverso fenomeno dello sviluppo delle comunicazioni immateriali e la "porosità" [8] che il territorio dimostra di avere dinanzi a tali flussi di informazioni e dati che superano le frontiere statuali, a volte semplicemente ignorandole, e che raggiungono le regioni più distanti. Per la verità non siamo di fronte a questioni non affrontate dalla dottrina internazionalistica dove si discute dei segni sempre più evidenti nel diritto internazionale di esercizio di forme di potere esercitate in maniera distaccata rispetto ad uno specifico territorio, fenomeno definito oggi come "deterritorializzazione" [9] del diritto internazionale; tema questo che affonda le sue radici in quegli autori che, a volte da una prospettiva profondamente diversa, hanno concepito il territorio non come un oggetto o un attributo essenziale della sovranità statuale ma, secondo una prospettiva funzionale, hanno definito il territorio solo come uno degli ambiti in relazione ai quali la sovranità esplica le sue funzioni, con frontiere definite in ragione del regime specifico di attività disciplinato, secondo un modello per alcuni applicabile al cyberspazio [10]. Se indubbia-

[7] Sul diritto all'oblio vedi, tra la vasta letteratura, il recente volume a cura di F. PIZZETTI, *Il caso del diritto all'oblio*, Torino 2013.

[8] È questo il termine utilizzato per alludere al fenomeno della progressiva perdita di controllo del territorio, da parte dello Stato, e delle competenze esercitate proprio a partire dal territorio. Se la relativizzazione del territorio produca anche una necessaria ridefinizione, dal punto di vista giuridico, dello Stato è il tema affrontato da H. RUIZ-FABRI, in *op. cit.*, p. 191 e ss.

[9] Per una descrizione della recente evoluzione del significato del territorio e delle frontiere nel diritto internazionale non solo riguardo ad Internet ma ad altri settori, come il diritto del commercio internazionale ed il diritto aerospaziale, sino a prefigurarne un approdo anche in questo caso di tipo funzionale, vedi E. MILANO, *The Deterritorialization of International Law*, vol. 2, 2013 in *Esil Reflections* reperibile *on line*: *http://www.esil-sedi.eu/node/311#_edn1*, in particolare p. 5: "*the distintive challenge for contemporary international law is...to adequately pursue a functional, global order, wich, on the one hand, protects and promotes basic public goods and fundamental human values, on the other, accomodates consitutional pluralism and diversity*". Per una definizione sintetica ma efficace della deterritorializzazione nel diritto internazionale vedi C. BRÖLMANN, *Deterritorializing International Law: Moving Away from the Divide between National and International Law*, in *Nollkaemper, Nijman (eds.), New Perspectives on the Divide between National and International Law*, ●UP, 2007, 84-109, ove il fenomeno viene considerato come "*the detachment of regulatory authority from a specific territory*".

[10] Riflessioni queste esposte da R. Quadri nel corso tenuto all'Aja di diritto

mente nel corso del dibattito sulla deterritorializzazione non sono mancati e non mancano elementi preziosi anche per valutare le implicazioni che questo fenomeno ha sul rispetto dei diritti umani, come per esempio la nozione di giurisdizione ai sensi dell'articolo 1 della Convenzione europea dei diritti dell'uomo (CEDU) utilizzata dalla Corte europea in relazione all'applicazione extraterritoriale della convenzione e che dimostrerebbe il passaggio da una competenza territoriale ad una competenza funzionale [11], le peculiarità spazio-temporali della rete rendono tuttavia più complesso valutare l'influenza, o con termine meno elegante ma forse più efficace, l'impatto che la Rete spiega nei riguardi della tutela dei diritti umani al punto da chiederci se sia necessario configurare nuovi diritti per tutelare gli "internauti" che li esercitano e ne fruiscono nel cyberspazio, soprattutto in considerazione della continua e non prevedibile evoluzione tecnologica che caratterizza la società digitale, o occorra invece un semplice ripensamento o una rilettura dei diritti esistenti in modo tale da calibrarli sulla funzione svolta nel cyberspazio. Il diritto europeo ed internazionale può contribuire a dare una risposta a tale domanda anche se rivolgere l'attenzione in primo luogo alle norme esistenti in tali ordinamenti, significa prendere in considerazione una regolamentazione pensata ed entrata in vigore in parte prima dell'avvento di Internet; ciò nonostante farvi riferimento costituisce un indispensabile punto di partenza per poter ricostruire, grazie anche all'analogia, una disciplina applicabile anche ai diritti in gioco sul *web* [12]. Alla logica di avvalorare una interpretazione analogica o una estensione dei principi maturati in tema dei diritti umani alle violazioni invece consumate in Rete, sembra ispirarsi, ad esempio, una recente risoluzione del Consiglio dei diritti umani delle

internazionale cosmico quando ritiene le attività extraatmosferiche spazialmente incoercibili e, per loro natura, non soggette alla funzione ed al fondamento della sovranità territoriale che "*n'est pour nous que le droit qu'a l'Etat d'exiger quel les autres Etas s'abstiennent d'interférer dans l'exercice qu'il fait de son pouvoir de gouverner. Cette abstention consiste à ne pas exercer des activités matérielles, coercitives ou autres dans certaines limites spatiales, mais l'espace ne vient ici en relief que comme une "modalité" de la protection d'un droit qui n'a pas pour objet l'espace*", in *Droit international cosmique*, Recueil des cours / Académie de Droit International de La Haye, 1959, III, pp. 509-597, in particolare p. 557. Impostazione dalla quale emerge un'interessante vicinanza di posizioni con le argomentazioni svolte da G. Scelle, in un suo scritto significativamente intitolato "*Obsession du territoire. Essai d'étude réaliste de droit international*" in *Symbolae J.H.W. Verzijl*, Nijhoff, 1958, pp. 347-361, quando l'autore francese individua la natura giuridica del territorio nel "*servir de limite aux competences gouvernamentales et administratives du système de Droit de la collectivité qui l'occupe*", non potendo considerarsi pertanto oggetto di proprietà dello Stato (p. 352).

[11] Corte europea diritti dell'uomo Al-Skeini c. Regno Unito, ricorso 55721/2007, sentenza del 7 luglio 2011; Catan ed altri c. Moldavia e Russia, ricorso 43370/04, 18454/06 8252/05, sentenza del 15 giugno 2010.

[12] J.J.A. Salmon, *Le raisonnement par analogie en droit international public*, in *Le droit des peuples à disposer d'eux-même. Méthodes d'analyse du droit international. Mélanges offerts à Charles Chaumont*, Pedone, 1984, pp. 495-525.

Nazioni Unite (NU) del 2012, che stabilisce che gli stessi diritti di cui godono le persone *off line* devono essere protetti anche *on line* [13], affermazione che sembra escludere la necessità di creare diritti "speciali" da far valere per le violazioni compiute *on-line* ma che merita una verifica svolta caso per caso: in effetti se per alcune fattispecie l'analogia può rivelarsi in grado di garantire lo stesso *standard* di protezione riconosciuto ai diritti al di fuori della Rete, ben potrebbero esservi situazioni nella quali gli ostacoli di ordine tecnico e tecnologico impediscono di ricostruire una disciplina completa ed adeguata per le violazioni commesse ai diritti *on line*, come anche potrebbero costituire semplicemente dei pretesti per non garantirli. Esempi in tal senso non mancano anche nella giurisprudenza della Corte europea dei diritti dell'uomo (EDU) toccando fattispecie di importanza diversa ma in ogni caso emblematiche di tali difficoltà: dalla impossibilità riconosciuta di eliminare grazie all'installazione di filtri informatici il fenomeno dello *spam*, per la mancanza di strumenti tecnici adeguati, con il risultato di lasciare gli utenti sprovvisti di tutela dinanzi ad un fenomeno ritenuto invasivo della vita privata [14], alle argomentazioni del governo turco nel recente caso Yldirim [15] che, per impedire l'accesso ad un solo sito Internet in quanto ritenuto offensivo della memoria di Ataturk, procedeva a bloccare l'accesso all'insieme dei siti del dominio Google, con una evidente violazione della libertà di espressione tutelata all'art. 10 della CEDU, giustificata proprio con l'impossibilità tecnica di intervenire sul solo sito incriminato. D'altra parte vi sono norme formulate in maniera tale da prestarsi agevolmente alla nuova realtà virtuale come l'art. 19 del Patto sui diritti civili e politici quando stabilisce che ogni individuo ha diritto alla libertà di espressione attraverso qualsiasi mezzo, frase dalla quale traspare chiaramente l'idea di una neutralità del mezzo utilizzato per esercitare tale diritto, in ciò rivelando un approccio aperto a qualsiasi soluzione tecnologica idonea ad assicurare tale diffusione, incluso naturalmente lo strumento di Internet [16]. O ancora, ed è questo forse l'elemento di maggiore novità, il rispetto del diritto alla

[13] Testualmente: "*the same rights that people have off line must also be protected online*" (ris. L13 del 6 luglio 2012).

[14] Corte europea Muscio c. Italia, ricorso n. 31358/03, sentenza 13 novembre 2007.

[15] Corte europea Ahmet Yldirim c. Turchia, ricorso 3111/10, sentenza 18 dicembre 2012.

[16] Nel senso indicato si sviluppa il *General Comment* n. 34 adottato dal Comitato per i diritti umani delle NU, nel corso della sua 102ma sessione, che ha esteso la tutela offerta dall'articolo 19 a "*all forms of audio-visual as well as electronic and internet-based modes of expression*" (par. 12), CCPR/C/GC/34; ma anche il *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*, Frank La Rue, UN Doc., A/HRC/17/27/ del 16 maggio 2011: "*By explicitly providing that everyone has the right to express him or herself through any media, the Special Rapporteur underscores that article 19 of the Universal Declaration of Human Rights and the Covenant was*

libertà di espressione "*regardless of frontiers*" che inevitabilmente si presta in maniera felice ad essere applicato ad una realtà a-territoriale come Internet, che fatica ad essere confinata in una dimensione esclusivamente nazionale, anche dal punto di vista delle garanzie ad esso applicabili [17]. È interessante notare che pur in mancanza di espliciti elementi testuali di "apertura" in favore della applicabilità alla realtà di Internet, come quelli citati, la necessità di garantire tutela ad uno dei diritti esposti a maggiori pericoli in Rete, il diritto di ogni individuo a non essere sottoposto ad interferenze arbitrarie o illegittime nella sua vita privata, codificato all'articolo 17 sempre del Patto NU sui diritti civili e politici, ha poi favorito una sua interpretazione diretta ad estendere le tutele previste dalla disposizione del Patto alle violazioni alla *privacy* perpetrate *on line*, ben al di là quindi dei tradizionali ambiti nei quali una compressione del diritto alla *privacy* si era sino ad allora consumato consentendo così al Comitato per i diritti dell'uomo delle NU, nel suo *General Comment* n. 16 [18], di delineare i rischi che possono correre tali diritti dinanzi alla costituzione di banche dati ed alla raccolta di informazioni, auspicando

drafted with foresight to include and to accommodate future technological developments through which individuals can exercise their right to freedom of expression. Hence, the framework of international human rights law remains relevant today and equally applicable to new communication technologies such as the Internet." (par. 21).

[17] *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*, cit.: "*Unlike any other medium, the Internet enables individuals to seek, receive and impart information and ideas of all kinds instantaneously and inexpensively across national borders*" (par. 67) ... ed ancora "*The Special Rapporteur emphasizes that there should be as little restriction as possible to the flow of information via the Internet, except in few, exceptional, and limited circumstances prescribed by international human rights law*" (par. 68). Sostanzialmente negli stessi termini *Report of the Special Rapporteur to the General Assembly on the right to freedom of opinion and expression exercised through the Internet*, *UN* Doc., A/66/290 del 20 agosto 2011. Lo stretto legame tra privacy e libertà di espressione è sottolineato, sempre dal Relatore Speciale Frank La Rue, nel suo *Report of the Special Rapporteur to the Human Rights Council on the implications of States' surveillance of communications on the exercise of the human rights to privacy and to freedom of opinion and expression*, UN Doc., A/HRC/23/40/del 17 aprile 2013 quando conclude che "*States cannot ensure that individuals are able to freely seek and receive information or express themselves without respecting, protecting and promoting their right to privacy. Privacy and freedom of expression are interlinked and mutually dependent; an infringement upon one can be both the cause and consequence of an infringement upon the other*" (par. 79).

[18] *General Comment* n. 16, *The right to respect of privacy, family, home and correspondence, and protection of honour and reputation* (Art. 17, del 08 aprile 1988, (Thirty-second session, 1988) ove si legge che "*Compliance with article 17 requires that the integrity and confidentiality of correspondence should be guaranteed de jure and de facto. Correspondence should be delivered to the addressee without interception and without being opened or otherwise read. Surveillance, whether electronic or otherwise, interceptions of telephonic, telegraphic and other forms of communication, wire-tapping and recording of conversations should be prohibited*", (par. 8), ed ancora; "*The gathering and holding of personal information on computers, data banks and other devices, whether by public authorities or private individuals or bodies, must be regulated by law. Effective measures have to be taken by States to ensure that information concerning a person's private life does not reach the hands of persons who are not authorized by law to receive, pro-*

in questi casi garanzie aggiuntive quali la codificazione, nelle legislazioni nazionali di settore, di un diritto dell'individuo a conoscere se e quali dati personali che lo riguardano sono stati raccolti e conservati ed a quali fini [19]. Questi spunti ricostruttivi dimostrano già un'attenzione al fenomeno Internet da parte degli organismi internazionali, pur scontando il dato di essere previsti in strumenti prevalentemente di *soft law* che tradiscono una certa ritrosia degli stati ad assumere impegni vincolanti in materia, ma è il contesto europeo [20] che ha offerto ed offre il banco di prova più serio per valutare l'efficacia delle tutele assicurate alla fruizione dei diritti umani sul *web*, ed in particolare al rispetto della vita privata [21]. Accanto ai due strumenti applicabili ad Internet quali la Convenzione sulla criminalità informatica, primo trattato internazionale sulle infrazioni penali commesse via Internet e su altre reti informatiche [22], e la Convenzione per la protezione delle persone nei confronti dei trattamenti automatici dei dati a carattere personale, primo strumento internazionale obbligatorio con lo scopo di proteggere le persone contro l'uso abusivo del trattamento automatizzato dei dati di carattere personale [23] ed aperta alla adesione degli Stati non membri del Consiglio d'Europa, aspetto che la rende l'unico strumento di diritto internazionale

cess and use it, and is never used for purposes incompatible with the Covenant", (par. 10).

[19] Per una prima configurazione del contenuto del diritto alla vita privata in relazione al trattamento elettronico dei dati personali, sempre il *General Comment* n. 16 cit.,:"*In order to have the most effective protection of his private life, every individual should have the right to ascertain in an intelligible form, whether, and if so, what personal data is stored in automatic data files, and for what purposes. Every individual should also be able to ascertain which public authorises or private individuals or bodies control or may control their files. If such files contain incorrect personal data or have been collected or processed contrary to the provisions of the law, every individual should have the right to request rectification or elimination*", (par. 10).

[20] Sul tema F.C. MAYER, *Europe and the Internet: the Old World and the New Medium*, in *European Journal of International Law*, 2010, pp. 149-169; Y. POULLET, *Vers la confiance: vues de Bruxelles: un droit européen de l'internet? Quelques considération sur la spécificité de l'approche réglementaire européene du cyberspace*, in *Le droit international de l'Internet. Actes du colloque organisé à Paris les 19 et 20 novembre 2001*, Bruxelles, 2002, pp. 133-176.

[21] La presenza, in questo caso, di strumenti vincolanti sia nell'ambito del Consiglio d'Europa che dell'U.E., con i relativi meccanismi di controllo giurisdizionale, hanno favorito un confronto continuo ed approfondito sul contenuto del diritto al rispetto della vita privata ed alla libertà di espressione, in un contesto che si pone al di fuori della dimensione puramente nazionale e con una casistica più ricca rispetto al diritto internazionale; ciò che peraltro spiega la scelta di anteporre il termine europeo ad internazionale anche nel titolo dell'articolo, soluzione questa che da un punto di vista sistematico risulterebbe altrimenti difficilmente giustificabile.

[22] Conclusa a Budapest il 23 novembre 2001 ed entrata in vigore il 1 luglio 2004, ad oggi registra 40 Stati parti della convenzione. Completata dal Protocollo addizionale relativo all'incriminazione di atti di natura razzista e xenofobica commessi a mezzo di sistemi informatici, firmato il 28 gennaio 2003 a Strasburgo ed entrato in vigore il 1 marzo 2006, ma non ratificato dall'Italia.

[23] La convenzione, detta convenzione 108, firmata a Strasburgo il 28 gennaio 1981 ed entrata in vigore il 1 ottobre 1985 che attualmente vede 46 Stati parti della stessa, si propone, tra l'altro, di favorire la cooperazione internazionale tra Stati in relazione al flusso transfrontaliero dei dati, impo-

vincolante a portata così ampia nella materia (ad oggi 42 ratifiche, con l'Uruguay) e che, proprio per tale caratteristica, potrebbe costituire la base giuridica per una regolamentazione globale del settore come auspicato da più parti, è l'applicazione alla realtà di Internet dei diritti contenuti nella Convenzione europea, in primis il diritto al rispetto alla vita privata e familiare *ex* art. 8 CEDU, che fa emergere un quadro normativo meno povero di strumenti europei ed internazionali di regolamentazione delle Rete, e dei diritti che lì si esercitano, di quello che generalmente si ritiene.

2. Diritto alla vita privata e protezione dei dati personali *on line* nel sistema CEDU.

È proprio nel contesto europeo che il diritto alla vita privata viene ben presto declinato quale diritto alla protezione dei dati personali, in seguito all'espansione delle attività svolte sul *web*, diventando così aspetto essenziale della tutela dei diritti umani *on line* al punto da far sorgere la questione se debba essere interpretato quale autonomo diritto fondamentale rispetto alla vita privata, come d'altronde prevede la Carta dei diritti fondamentali. La nozione relativa di *privacy*, non definita volutamente in maniera esaustiva dalla Corte europea dei diritti dell'uomo [24], ha poi favorito una sua profonda evoluzione se consideriamo che da una concezione iniziale, quale diritto ad essere lasciati soli nella intimità della propria vita privata e familiare, si è giunti a configurarla come diritto per l'individuo di stringere e sviluppare rapporti con i propri simili, di autodeterminarsi in relazione a tutti gli ambiti nei quali si esprime la propria personalità che assume la forma di diritto all'autodeterminazione informativa una volta entrata in contatto con il *web*, sino ad essere intesa oggi quale potere di controllo di cui gode l'individuo sulle modalità e le condizioni in base alle quali le informazioni che lo riguardano sono conservate ed archiviate. Tutela della *privacy* che, nel rinnovato contesto del cyberspazio, deve fare i conti con forme di ingerenza che prescindono dalla natura pubblica o privata del soggetto che le compie e che, dinanzi alla capacità che i privati dimostrano di poter insidiare la *privacy* sul *web*, tramite le obbligazioni positive imposte agli Stati mira ad estendere la sfera di applicazione delle garanzie previste all'art. 8 CEDU ai rapporti intersoggettivi, senza dover così necessariamente ricorrere, per riconoscere l'efficacia di tali disposizioni anche nei confronti dei privati, alla controversa nozione dell'"efficacia orizzontale" della

nendo delle limitazioni per i flussi diretti verso stati in cui non esiste alcuna protezione equivalente.

[24] X e Y c. Paesi Bassi, ricorso 8978/80, sentenza del 26 marzo 1985; più di recente, Pretty c. Regno Unito, ricorso 2346/2002, sentenza del 24 aprile 2002.

Convenzione [25]. Una efficacia della tutela dei diritti degli utenti nei confronti di altri privati sulla Rete, i cd. intermediari e cioè motori di ricerca e dei *social network*, che viene così a dipendere in buona sostanza dall'applicazione anche a questi ultimi dei criteri e dei limiti in base ai quali le ingerenze alla *privacy* ed alla protezione dei dati personali possono essere considerate consentite o legittime, misure poste in un bilanciamento continuo con le esigenze necessarie ad una società democratica, ponderazione resa possibile in ragione della natura derogabile e non assoluta del diritto in questione. Si tratta di principi elaborati dalla Corte che muovono dal ritenere la semplice conservazione delle informazioni in *files* una interferenza, ai sensi dell'articolo 8 della CEDU, non avendo alcuna influenza, ai fini della definizione della stessa, l'uso successivo che viene fatto delle informazioni così raccolte [26]. E pur quando si dovesse trattare di ingerenza consentita necessaria ad una società democratica e prevista per legge, la conservazione e memorizzazione dei dati personali potrà ammettersi solo per un adeguato periodo di tempo, non potendo essere illimitata costituendo la mancanza di un termine certo previsto per legge una violazione della Convenzione, ed in ogni caso soggetta ad un diritto alla cancellazione dei dati [27]. Chiaramente ciò implica una valutazione in termini di proporzionalità della durata della conservazione dei dati rispetto allo scopo del loro trattamento, alla gravità dei comportamenti che ne sono all'origine non potendosi mai trattare in ogni caso di un potere di conservazione a carattere generale ed indifferenziato [28]. Principi che hanno indotto la Corte a ritenere non sussistente la violazione dell'art. 8 in relazione ad

[25] X e Y c. Paesi Bassi, sentenza cit.: "*La Cour rappelle que si l'article 8 a essentiellement pour objet de prémunir l'individu contre les ingérences arbitraires des pouvoirs publics, il ne se contente pas de commander à l'Etat de s'abstenir de pareilles ingérences: à cet engagement plutôt négatif peuvent s'ajouter des obligations positives inhérentes à un respect effectif de la vie privée ou familiale (arrêt Airey 9 octobre 1979). Elles peuvent impliquer l'adoption de mesures visant au respect de la vie privée jusque dans les relations des individu entre eux*". Per una questione relativa ad internet K.U. c. Finlandia, ricorso n. 2872/02, sentenza del 2 ottobre 2008.

[26] Amman c. Svizzera, ricorso n. 27798/95, sentenza del 16 febbraio 2000: "*The storing by a public authority of information relating to an individual's private life amounts to an interference within the meaning of Article 8. The subsequent use of the stored information has no bearing on that finding*". Per una rassegna delle principali sentenze della Corte europea dei diritti dell'uomo relative ad Internet vedi il rapporto preparato dalla divisione ricerca della Cancelleria del 2011 reperibile *on line*: *www.echr.coe.int*.

[27] S. e Marper c. Regno Unito, ricorso n. 30562/04, sentenza Grande Camera del 4 dicembre 2008.

[28] Non è solo il fattore temporale a determinare i requisiti ai quali è subordinata la legittimità della conservazione dei dati; nel caso riportato alla nota precedente e relativo alla conservazione in un database della impronte digitali e genetiche del ricorrente, il carattere generale ed indifferenziato del potere di conservazione dei dati attribuito alle autorità statali, a prescindere dalla natura e dalla gravità delle infrazioni commesse dalla persona, semplicemente per il fatto di essere sospettata ed indipendentemente da una sua condanna o dalla sua età, oltre che alla mancanza della possibilità di ottenerne la cancellazione o la distruzione, ha indotto la Corte a ritenere che

ipotesi delittuose particolarmente gravi, tali da giustificare la loro conservazione in un data base per 30 anni [29], mentre in altro caso ha ritenuto che la conservazione delle impronte digitali di un cittadino francese soggetto a due indagini relative ad alcuni libri rubati integrasse una sproporzionata interferenza nella vita privata del ricorrente, considerata anche la lievità della infrazione commessa [30]. In linea di principio, quindi, non vi è motivo per escludere che tali criteri, ai quali dovrebbero ispirarsi anche le legislazioni statali, diventino parametro di legittimità anche delle misure di ingerenza alla *privacy* messe in atto nel cyberspazio, con l'obiettivo di assicurare cosi garanzie minime agli internauti che vedono i loro dati personali trattati sul *web*: la nozione relativa di *privacy*, che non ha prodotto una tipizzazione delle forme di ingerenza né ha fatto dipendere la legittimità o meno dell'esercizio di tale potere dalla natura pubblica o privata del soggetto che la mette in atto, si pensi alla giurisprudenza relativa alle attività di controllo o monitoraggio da parte dei datori di lavoro, può dilatarsi facilmente sino a comprendere tali nuove forme di interferenza nella vita privata [31].

3. Ruolo e responsabilità degli intermediari nella protezione dei dati personali in Europa.

Ma l'aspetto che rende problematico estendere alle attività svolte sul *web* le tutele alla vita privata previste per le situazioni *off line* e che tocca oggi un punto cruciale dello *standard* assicurato ai tali diritti sul *web*, riguarda il ruolo che possono svolgere le obbligazioni positive nell'assicurare in maniera efficace la protezione del diritto alla vita privata, quando poste in relazione al tipo di attività che viene svolto sul *web* da coloro che sono ormai i protagonisti della protezione dei dati personali, e dunque inter-

nella fattispecie mancasse quel giusto equilibrio e bilanciamento tra interessi pubblici e privati tale da giustificare una misura necessaria in un società democratica, e quindi una forma di ingerenza ammessa (di cui al par. 2 dell'art. 8), dunque misure in definitiva costituenti un attacco sproporzionato al diritto al rispetto della vita privata. Nello stesso senso Rotaru c. Romania, ricorso n. 28341/95, sentenza del 4 maggio 2000, Grande Camera.

[29] Nel caso Bouchacourt c. Francia e Gardel c. Francia, ricorso n. 53335/06 del 17 dicembre 19209, concernente l'inserimento e la conservazione dei dati in un data base dedicato ai delitti a sfondo sessuale, di tre soggetti condannati per violenza nei confronti di una minorenne da parte di adulti, aventi una posizione di autorità nei confronti della vittima, lasso di tempo e termine non considerati sproporzionati in relazione agli scopi perseguiti, la prevenzione dei crimini di tale gravità appunto.

[30] M.K. c Francia, ricorso n. 19522/09, sentenza del 18 aprile 2013.

[31] Nel valutare la legittimità dell'attività conservazione, controllo e monitoraggio dei dati nei confronti di una dipendente da parte del proprio datore di lavoro, la Corte non ha perso occasione di precisare la "neutralità" del mezzo utilizzato per ingerirsi nella vita privata, di fatto operando una completa assimilazione tra l'utilizzazione del telefono, delle mail e dell'uso di Internet, anche per quanto riguarda la necessità di una loro salvaguardia nell'uso, vedi Copland c. Regno Unito, ricorso n. 62617/00, sentenza del 3 aprile 2007.

mediari privati, motori di ricerca, *social network*. Si tratta infatti di attività che consentono loro di acquisire automaticamente i dati personali degli utenti quando inseriscono, ad esempio, dei termini di ricerca nei motori di ricerca, che una volta raccolti e trattati, permettono di delineare gusti ed eventuali comportamenti dell'utente volti ad orientare i fornitori di servizi ed i motori di ricerca nella scelta delle offerte da sottoporgli in occasione dell'accesso ai servizi, ad esempio di prenotazione di alberghi o viaggi in rete. Con servizi solo apparentemente gratuiti, poiché i dati e le informazioni che sono forniti dall'internauta al momento della fruizione di tali servizi, rappresentano la vera moneta di scambio ed il prezzo che viene corrisposto ai motori di ricerca, in esecuzione di una sorta di tacito accordo frutto della semplice interazione sul *web*. Ed è questa la ragione per la quale i dati cosi raccolti sono da alcuni considerati come il nuovo "petrolio" della società digitale. D'altra parte anche il ruolo fondamentale svolto dai *social network* che gestiscono i dati personali postati in tali servizi suscita non poche riflessioni circa la protezione dei dati personali. È cosa nota infatti che, con una certa continuità, ormai gli intermediari sono destinatari di richieste di accesso affinché siano forniti dati ed informazioni immessi in Rete dagli utenti, sia da parte di privati che di autorità pubbliche. Ora sin quando la possibilità di disporre da parte dei *providers* o dei *social network* di tali dati ed informazioni dell'utente trova la sua fonte, se non in un atto legislativo, in clausole contrattuali, come quelle che abilitano ad esempio i gestori di *social network* a cancellare dati ed informazioni dell'utente o ad escluderlo dal *social network* in base al proprio insindacabile giudizio e per qualsiasi motivo, o il diritto che i motori di ricerca si riservano di conservare i dati senza limiti di tempo, la loro legittimità alla luce dei criteri che abbiamo visto in precedenza, può senz'altro essere scrutinata, data l'ampiezza della nozione di obbligazioni positive accolta dalla Corte; ampiezza che si estende sino al punto da prevedere, per gli organi statali ivi compresa l'autorità giudiziaria, l'obbligo di impedire l'effettività di clausole contrattuali che comportino la violazione di un diritto fondamentale [32], considerando incompatibile con gli obblighi derivanti dalla convenzione anche semplicemente il tollerare l'applicazione di clausole contrattuali in grado di violare i diritti umani [33]. Attribuendosi così la Corte il ruolo di fatto di garante della CEDU anche nell'ambito di con-

[32] Sorensen Rasmussen c. Danimarca, ricorsi n. 52562/99 e 52620/99, Sentenza 11 gennaio 2006 Grande Camera.

[33] Per il ruolo che le obbligazioni positive possono svolgere nel sistema CEDU in presenza di clausole contrattuali ritenute illegittime, F. DONATI, *Condizioni di utilizzo dei* Social Network *e diritti fondamentali*, in *L'informazione il percorso di una libertà*, Volume II a cura di P. CARETTI, pp. 101-113, Firenze 2012.

troversie di natura privatistica. Di ben diversa natura appare invece lo *standard* di protezione dei dati personali nel caso di attività di intermediari non contenute in una regolamentazione di natura contrattuale, né tanto meno legislativa che, come abbiamo visto, se non altro tramite le obbligazioni positive consente una qualche forma di intervento qualora la disciplina in essa prevista si rivelasse contraria alle norme CEDU. In effetti sempre più frequentemente, al punto oramai da apparire una prassi generalizzata, i motori di ricerca procedono nell'ambito delle loro attività a trattare i dati degli utenti senza alcun consenso da parte dell'interessato, rapporti instaurati, come visto, in forza della semplice interazione sul *web*, spesso all'insaputa degli internauti ignari del trattamento dei loro dati. Sono attività di profilazione o combinazione ed incrocio tra di loro dei dati, che vengono tratti dai diversi servizi utilizzati dagli utenti, al fine di implementare altri servizi, come la pubblicità [34]. Poiché ogni attività di tal tipo svolta dai *providers* richiede necessariamente la conservazione dei dati degli utenti circostanza che, di per sé, integra una ingerenza nella vita privata, ecco che tale attività dovrebbe essere accompagnata dal rispetto di quei criteri in presenza dei quali solo può essere ritenuta legittima mentre, in realtà, il loro trattamento avviene sovente senza l'indicazione di limiti di tempo, soprattutto nel caso di memorizzazione e indicizzazione da parte dei motori di ricerca delle pagine *web* e di creazione di una copia cache della pagina, con riferimenti non chiari circa la finalità specifica del loro trattamento e dunque in assenza del rispetto del principio di proporzionalità, senza la previsione per l'interessato del diritto di opporsi al trattamento, aspetti non regolamentati in altro modo. Queste criticità sono al centro di un'indagine condotta dalla *Commission Nationale de l'Informatique et des Libertés* (CNIL), autorità garante francese per conto delle autorità di protezione europee nei confronti di Google, che ha ad oggetto proprio la *policy privacy* di società che gestiscono motori di ricerca e che è ancora in corso [35]. Dinanzi a tale stato di cose anche gli strumenti della Convenzione europea possono rivelarsi efficaci solo fino ad un certo punto, poiché risulta difficile assi-

[34] Di frequente la stessa natura dei dati trattati non è chiara e quando sono previsti meccanismi di *opt-out* rispetto al loro trattamento, le modalità per poterne usufruire sono macchinose ed inefficaci per cui l'unico rimedio possibile in alcuni casi è non avvalersi del servizio.

[35] Reperibile *on line: http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2012/20121016_press_release_google_privacy_cnil_en.pdf*. In alcuni paesi come in Germania sono state previste alcune garanzie per gli utenti tra le quali la esclusione della combinazione dei dati estratti dai diversi servizi, l'obbligo di concludere uno specifico contratto tra il motore di ricerca e il website, la possibilità per l'utente di rendere automaticamente anonimo il proprio indirizzo IP condiviso con il motore di ricerca, ma si tratta di iniziative sporadiche e che lasciano il quadro delle garanzie a livello europeo frammentato.

curare agli utenti del *web* il godimento effettivo del diritto alla protezione dei dati personali in presenza di prassi e comportamenti ritenuti illegittimi ma che in mancanza di una qualsiasi loro base giuridica, come accade nel caso esistano invece condizioni contrattuali in grado di far emergere e cristallizzare in un testo vincolante comportamenti contrari alla *privacy*, sfuggono a qualsiasi dichiarazione e valutazione di illegittimità e inefficacia ai sensi della convenzione, anche se indirettamente per il tramite dello Stato responsabile. È questo un limite, forse, oltre il quale il ricorso all'analogia non può spingersi ed essere di ausilio per disciplinare tali fattispecie [36]. Al più, se si dovesse registrare una crescita significativa del numero di ricorsi depositati a Strasburgo relativi alla violazione dell'art. 8 per i motivi che stiamo esaminando, *trend* in crescita che peraltro già esiste e che non riguarda solo l'Italia, non si potrebbe escludere l'adozione da parte della Corte di sentenze pilota grazie alle quali, una volta identificato il problema sistemico o il malfunzionamento dell'ordinamento interno all'origine della violazione strutturale alla convenzione, in questo caso ravvisata proprio nell'assenza o inadeguatezza delle legislazioni nazionali a tutela della vita privata, disporre a carico dello Stato o degli Stati interessati dalla procedura, l'adozione di misure generali per la loro risoluzione in pratica l'adozione di una legge in materia [37]. Se dunque si vuole evitare che l'utente dinanzi a queste nuove forme di ingerenza versi in quella condizione che la Corte europea, quando prese atto della impossibilità di fronteggiare il fenomeno dello *spam*, aveva delineato con un'affermazione che pecca forse di eccessivo realismo, di utilizzatori del sistema che una volta connessi alla rete Internet non godono più di una protezione effettiva della loro vita privata, esponendosi in quel caso alla ricezione di messaggi, immagini ed informazioni spesso non sollecitate [38], la risposta a queste nuove forme di ingerenza sembra passare necessariamente per l'adozione di una legislazione da parte dei singoli Stati in materia, volta a regolamentare dettagliatamente i casi di responsabilità nei quali può incorrere l'intermediario che tratta i dati o le informazioni per-

[36] Considerato che anche nel caso in cui lo Stato dovesse essere dichiarato inadempiente agli obblighi positivi derivanti dalla convenzione europea per aver tollerato condizioni contrattuali contrarie alla convenzione, ciò non si tradurrebbe in un'affermazione diretta di responsabilità degli intermediari, dovendosi a tal fine attendere un'eventuale iniziativa a livello interno anche di carattere legislativo.

[37] Sulla nozione di violazione strutturale B. NASCIMBENE, *Violazione "strutturale", violazione "grave" ed esigenze interpretative della Convenzione europea dei diritti dell'uomo*, in *Rivista di diritto internazionale privato e processuale*, 2006, pp. 645-656; F. SALERNO, *Le modifiche strutturali apportate dal Protocollo n. 14 alla procedura della Corte europea dei diritti dell'uomo*, in *Rivista di diritto internazionale privato e processuale*, 2006, pp. 377-398, in particolare pp. 384 e ss.; U. VILLANI, *Il Protocollo n. 14 alla Convenzione europea dei diritti dell'uomo*, in *La comunità internazionale*, 2004, pp. 487-501, in particolare pp. 490 e ss.

[38] Muscio c. Italia, sentenza cit.

sonali. D'altronde se le misure di ingerenza adottate dai pubblici poteri per essere ammesse devono ispirarsi ai criteri della appropriatezza, della proporzionalità ed esser necessarie in una società democratica, riesce difficile non immaginare che simili principi debbano guidare l'azione ed i comportamenti dei *providers*, quando esercitano loro forme di ingerenza che, peraltro, non sono giustificate da un interesse generale [39]. In definitiva l'attuale *legal black hole* non sembra favorire per alcuni versi gli stessi *providers* i quali, in assenza di riferimenti normativi chiari sul punto e con una tendenza in atto che va verso la loro identificazione con la figura del responsabile del trattamento dei dati personali, sono più facilmente soggetti a quelle oscillazioni giurisprudenziali che in alcuni casi hanno portato ad interpretare in maniera eccessivamente estensiva la loro responsabilità, come nel caso *Pirate Bay* o *Vividown c. Google* [40] configurando in questi casi a loro carico sostanzialmente un obbligo di controllo preventivo e generalizzato su tutti i contenuti, informazioni e dati immessi dai propri utenti e giustificando così interventi di natura censoria sui contenuti immessi in rete, attività che potrebbe implicare a propria volta una ingiustificata limitazione dei diritti fondamentali degli utenti.

4. Prospettive di riforma della protezione dei dati personali nella U.E.

Parzialmente differente si presenta lo scenario europeo a livello di Unione europea dove già nel Preambolo troviamo il richiamo alla necessità di rafforzare la tutela dei diritti fondamentali alla luce dell'evoluzione della società, del progresso sociale e degli sviluppi scientifici e tecnologici, riferimento che viene sviluppato nel Trattato sul Funzionamento dell'U.E. di Lisbona che, all'art. 16, contempla espressamente un autonomo "diritto alla protezione dei dati di carattere personale"; la disposizione è stata interpretata nel senso di predisporre una tutela dei diritti individuali che opera *erga omnes*, obbligando al rispetto della disposizione tanto i soggetti investiti di pubbliche funzioni, istituzioni ed

[39] È una strada questa già intrapresa dalla stessa Corte che in situazioni analoghe come nel caso Copland c. Regno Unito citato e relativo al controllo della mail, delle telefonate e di Internet da parte del datore di lavoro, ha ritenuto una violazione della convenzione la mancanza di una legislazione statale volta a disciplinare i casi di ingerenza nella vita privata, ammessi e consentiti, affermando così un principio che peraltro esclude che si possa far ricorso, per colmare le lacune esistenti in materia, a fonti di secondo grado come regolamenti (pensiamo al ruolo delle autorithy in tal senso), con i quali determinare ad esempio tempi e modi di cancellazione dei dati, modalità di conservazione degli stessi ecc..

[40] Per le implicazione che questa decisioni produce per la tutela dei diritti fondamentali, secondo una prospettiva costituzionale, vedi il recente volume a cura di E. Apa e O. Pollicino, *Modeling the Liability of the Internet Service Providers: Google vs. Vivi Down*, Milano 2013.

organismi dell'Unione europea e nazionali, tanto da parte di qualsiasi soggetto privato le cui attività possono interferire con il diritto in questione [41]. Questa interpretazione volta a riconoscere la più ampia sfera di applicazione al diritto, anche in ordine alla sua efficacia orizzontale, giustifica l'istituzione in favore dell'Unione di una vera e propria competenza che è stata prontamente esercitata con la proposta di regolamento del Parlamento europeo e del Consiglio concernente la tutela delle persone fisiche con riguardo al trattamento dei dati personali e la libera circolazione di tali dati [42] attualmente in discussione al Consiglio, in sostituzione della direttiva 95/46, che si propone di estendere alla società digitale i principi maturati in materia di protezione di dati personali. Al centro di un acceso dibattito a Bruxelles, per quanto concerne il profilo della tutela degli "internauti" nei confronti dei soggetti economici che operano in Rete e non solo nei riguardi degli stati, una volta adottato l'atto farà già registrare un notevole passo in avanti per il solo fatto di disciplinare la materia tramite lo strumento del regolamento, e non con direttiva, offrendo così opportunità di tutela ai privati-internauti nei confronti dei *service providers*, come anche di tutti coloro che rivestiranno la qualifica di responsabili di trattamento personale, in virtù della sua applicabilità ai rapporti intersoggettivi [43].

Anche la Carta dei diritti fondamentali, all'art. 8, prevede il diritto di ogni individuo alla protezione dei dati personali, in maniera distinta e separata rispetto al diritto al rispetto della vita privata, previsto all'articolo precedente, specificando però il principio che i dati devono essere trattati secondo lealtà, per finalità determinate ed in base al consenso della persona interessata o ad un altro fondamento legittimo previsto dalla legge. Sembrerebbe questa una prima risposta a livello UE alle preoccupazioni per la *privacy* che abbiamo visto in precedenza caratterizzare l'attività dei motori di ricerca, quando trattano i dati anche senza il consenso degli utenti, poiché condizionare qualsiasi tipo di trattamento dei dati al solo consenso dell'interessato sembra voler favorire una loro tutela dinamica, con la possibilità per l'utente di seguire la loro circolazione in rete consacrando quindi quella concezione della vita privata intesa, nel mondo di Internet, come autodeterminazione informativa. È questa d'altronde la direzione nella quali si muove l'art. 17 della proposta di

[41] B. CORTESE, *La protezione dei dati di carattere personale nel diritto dell'Unione europea dopo il Trattato di Lisbona*, in *Il diritto dell'Unione europea*, 2013, pp. 313-335.

[42] Regolamento generale sulla protezione dei dati, COM (2012) 11 final. 2012/0011 (COD), Bruxelles 25 gennaio 2012.

[43] Per le prospettive di riforma legate al Regolamento generale vedi O. POLLICINO e M. BASSINI, *Diritto all'oblio: i più recenti spunti ricostruttivi nella dimensione comparata ed europea*, in F. PIZZETTI, *op. cit.*, pp. 185 e ss.; in particolare per il *legal framework* europeo vedi pp. 191-194.

Regolamento generale sulla protezione dei dati, attualmente in discussione in Consiglio ove viene stabilito, in ciò non discostandosi significativamente dalla precedente direttiva 95/46 CE, che l'interessato ha il diritto di ottenere dal responsabile del trattamento la cancellazione di dati personali che lo riguardano e la rinuncia a un'ulteriore diffusione di tali dati [44], in presenza di una serie di motivi tra i quali vanno annoverati principalmente i casi nei quali i dati non sono più necessari rispetto alle finalità per cui sono stati raccolti, o l'interessato revoca il consenso su cui si fonda il trattamento, oppure il periodo di conservazione dei dati autorizzato è scaduto e non sussiste altro legittimo motivo per trattarli. Congiuntamente al rafforzamento della posizione dell'interessato il Regolamento generale delinea un sistema di responsabilità sempre maggiore nei riguardi dei responsabili del trattamento dei dati [45], soprattutto garantendo l'*enforcement* del diritto alla cancellazione dei dati imponendo ai responsabili del trattamento, spesso *provider*, non solo di cancellare i dati in loro possesso, a richiesta dell'interessato, ma anche di comunicare a terzi, ai quali tali dati sono stati trasferiti, la richiesta di cancellazione, per rimuoverli anche se sono stati già pubblicati come accade nella gran parte dei casi sulla rete [46]. In definitiva l'impianto complessivo del Regolamento disegna l'abbandono dell'attuale regime [47] di *opt-out* che vuole i dati dell'utente, in mancanza di una sua espressa richiesta, appartenenti al fornitore a quella dell'*opt-in*, per cui i dati invece apparterrebbero all'utente solamente, rimanendo nella sua piena disponibilità la decisione circa il loro utilizzo. Le implicazioni economiche sono notevolissime: concepito in questi termini il diritto alla cancellazione dei dati in favore dell'utente, lo stesso trattamento dei dati a fini di marketing o commerciali da parte dei fornitori di servizi e dei motori di ricerca potrebbe essere messo in discussione rendendo il loro possesso provvisorio, in quanto condizionato alla possibile revoca dell'utente, una volta venuto meno il titolo per essere trattati. Impatto economico che sarà amplificato dall'ambito di applica-

[44] In particolare in relazione ai dati personali resi pubblici quando l'interessato era un minore.

[45] Una parte significativa di questi temi è attualmente al centro di una recente procedura di rinvio pregiudiziale pendente dinanzi alla Corte di Giustizia dell'Unione europea (causa C-131/2012), sollevata dal Tribunale di Madrid 9 marzo 2012, in merito ad una controversia insorta tra l'Autorità spagnola per la protezione dei dati e Google Spain/Google Inc circa la responsabilità dei fornitori di servizi di motore di ricerca per il fatto che nelle pagine *web* da loro trattate compaiano dati personale. Il 25 giugno 2013 sono state rassegnate le conclusioni da parte dell'Avvocato generale ma la causa sarà decisa sulla base della direttiva 95/46, destinata ad essere superata una volta adottato il Regolamento generale, come abbiamo visto.

[46] Di fatto cancellando i *link*.

[47] Che come abbiamo visto si basa essenzialmente sulla semplice interazione priva di un consenso validamente espresso o su un tacito accordo, nel migliore dei casi, in virtù del quale l'utente cede spesso inconsapevolmente i propri dati personali processati per fini ad esso non conosciuti, a fronte dei servizi che gli sono offerti sul *web*.

zione che avrà il Regolamento in quanto all'art. 3 recepisce il cd. principio del *target* in forza del quale la normativa europea viene applicata anche quando il trattamento è effettuato da un titolare che ha lo stabilimento fuori dal territorio dell'UE qualora il trattamento riguardi "l'offerta di beni o la prestazione di servizi ai residenti dell'UE" o se il trattamento riguarda "il controllo del loro comportamento" rendendo così irrilevante il luogo dove si effettua il trattamento quando questo interessa un residente nel territorio dell'UE, aggiungendosi al principio dello stabilimento. La portata che la disposizione ha sulla determinazione della legge applicabile la si può cogliere appieno sol che si consideri che l'applicazione della legge del luogo ove si svolge il trattamento è stato il principale argomento difensivo dei *service providers* statunitensi per evitare di assoggettarsi alla legislazione europea ed alla giurisdizione degli Stati membri, avendo tali società la sede appunto al di fuori del territorio europeo e specificamente negli USA, argomento questo utilizzato anche nel rinvio pregiudiziale attualmente pendente a Lussemburgo promosso dal Tribunale di Madrid nella controversia sorta tra l'Autorità garante dei dati spagnola e Google [48].

5. Conclusioni.

Si va dunque nel sistema UE, con il rafforzamento del consenso, verso un diritto di proprietà dei dati personali, secondo una visione cara a molti autori che sposano una analisi economica del diritto [49], che implica il diritto a disporne vendendoli e commercializzandoli fissando così in via autonoma il livello ottimale di protezione della propria vita privata, sfuggendo a quella che è stata definita una visione paternalistica dello Stato? A mio avviso non c'è motivo di abbandonare la nozione relativa di *privacy* coniata dalla Corte europea che le ha permesso, nei limiti consentiti dalle modalità di funzionamento di quel sistema, di confrontarsi con le nuove forme di ingerenza della società digitale e ricorrere quindi al bilanciamento tra i diritti messi in gioco dal *web*; bilanciamento che però questa volta dovrà considerare il diverso contesto dell'U.E. [50] e della Carta che ci obbliga a fare i conti non solo con la libertà di espressione, con la tutela del

[48] Giudizio citato, di cui alla nota 45.

[49] R.A. Posner, *Economic Analysis of the Law*, New York, 1998, p. 46 e ss. dove la vita privata ed i dati personali sono ritenuti un settore del diritto di proprietà.

[50] È il problema del bilanciamento dei diritti in gioco che però potrebbe costituire lo strumento attraverso il quale rileggere o ripensare i diritti alla luce delle novità legate alla Rete. Per rimanere alla Carta gli articoli 8 e 7 dovranno essere "bilanciati" con la libertà di espressione e d'informazione di cui all'art. 11 e la libertà di impresa di cui all'art. 16. Ma non vanno trascurati in quest'opera di bilanciamento che appare necessaria, altri diritti con i quali occorre diciamo "fare i conti" e cioè il diritto di proprietà ed, in particolare, la tutela della proprietà intellettuale (articolo 17, paragrafo 2); il divieto di qualsiasi forma di

consumatore, la libertà di impresa, il diritto di proprietà ma soprattutto con l'art. 1 della Carta che riconosce che "la dignità umana è inviolabile. Essa deve essere rispettata e tutelata". Il richiamo ad un tale valore fondamentale spinge ad interpretare il diritto del singolo a decidere in prima persona sulla cessione e l'uso dei dati personali, e cioè la sua autodeterminazione informativa, come una delle declinazioni possibili della tutela della dignità dell'uomo, espressione di quel legame stretto e diretto tra protezione dei dati personali, pieno sviluppo della personalità e dignità umana che la Corte costituzionale federale tedesca aveva già delineato sin dal 1983 [51], e ribadito di recente nel 2012 [52], che pone certamente dei limiti alla piena negoziabilità dei dati escludendo che il consenso di per sé possa considerarsi condizione sufficiente per disporne illimitatamente, ad opera dell'utente diventato proprietario, quando in contrasto con il rispetto della dignità umana [53]. Dinanzi a fenomeni recenti apparsi sul *web* come quello di una recente *start up* di Minneapolis che consente di mettere *on line* il proprio codice genetico ed ogni volta che una società lo consulta l'utente, che ha ceduto i propri dati, riceve una piccola somma, ad esempio una società attiva nel settore dell'alimentazione che vuole personalizzare una pubblicità di un determinato prodotto perché risulta dal codice genetico ceduto un'insofferenza di quella persona al glutine, realizzando cosi quella che è stata definito il primo "*member-controlled human genetic marketplace*", riconoscere che la protezione dei dati personali affonda le proprie radici in valori fondamentali che sono stati positivizzati nella Carta dei diritti fondamentali, e non la rendono assimilabile in tutto ad un diritto di proprietà in quanto tale alienabile, non sembra oggi una acquisizione di poco conto. In conclusione se una delle poche considerazioni generalmente con-

discriminazione fondata, tra l'altro, sulla razza, l'origine etnica, le caratteristiche genetiche, la religione o le convinzioni personali, le opinioni politiche o di qualsiasi altra natura, la disabilità, o l'orientamento sessuale (articolo 21); i diritti del minore (articolo 24); il diritto a un elevato livello di protezione sanitaria (articolo 35); il diritto d'accesso ai documenti (articolo 42); il diritto a un ricorso effettivo e a un giudice imparziale (articolo 47).

[51] Sentenza del 15 dicembre 1983, *BVerGE*, 65, 01. Interpretazione questa in linea con la Legge fondamentale che prevede, anch'essa, al primo articolo la tutela della dignità dell'uomo definita come intangibile e che pone a carico di ogni potere statale il dovere di rispettarla e proteggerla. Per una lettura del legame tra il diritto al rispetto ed alla protezione della dignità, diritto allo sviluppo della persona e protezione dei dati personali: Y. Poullet, A. Rouvroy, *Le droit à l'autodétermination informationelle et la valeur du développement personnel. Une réévalutation de l'importance de la vie privée pour la democratie*, in K. Benyekhlef e P. Trudel, *op. cit.*, Montréal, 2009, pp. 157-222, in particolare pp. 173 e ss.

[52] Sentenza 2 gennaio 2012 *BVerGE*, 1299, 05.

[53] Per un esame della tutela della dignità dell'uomo quale principio fondante i diritti strettamente connessi allo sviluppo della persona, incluso il diritto all'oblio e l'"autodeterminazione informatica", vedi T. Frosini, *Il diritto all'oblio e la libertà informatica*, pp. 85-96, in particolare pp. 94-95, in a cura di F. Pizzetti, *op. cit.*, Torino, 2013.

divise sulla globalizzazione, con sfumature e accenti diversi, vuole che la globalizzazione, quale ne sia l'esatto significato, ha comportato e comporta una sottrazione di aspetti significativi della sovranità degli Stati nazionali, senza che ciò sia stato ancora compensato da un sistema di *governance* in grado di influire efficacemente su tali quote di sovranità "liberate"; se quindi il processo di globalizzazione viene inteso, come è stato detto, come una "perdita non compensata o non adeguatamente compensata" [54], il quadro offerto dagli strumenti europei ed internazionali di tutela dei diritti umani sul *web*, e che si è cercato di illustrare, induce a ritenere che se non ci troviamo di fronte alla piena compensazione di questa perdita, tali strumenti di tutela rappresentano almeno un primo passo affinché la compensazione di questa perdita sia un po' più adeguata.

Abstract

The paper focuses on the greatest challenge to privacy legislation that arises because, while the Internet is virtually borderless, legislative approaches differ not only from country to country, but also from European to International system. The Article presents an analysis of the existing Human Rights Instruments as it applies to new technologies, particularly on the Article 19 of the International Covenant on Civil Rights, that intended to include later-developed technologies such as the Internet. Further the essays aims to investigate the extent to which individual privacy, and personal data, is protected by European Convention of Human Rights and the Strasbourg Court. Finally the authors examines the main issues on the responsibility of non State Actors for personal data protection violations, considering that data protection is now a fundamental right guaranteed according to the Treaty of Lisbon and the Charter on Fundamental Rights.

54 In P. CARETTI, *I diritti e le garanzie*, Relazione Convegno annuale AIC, "Costituzionalismo e globalizzazione", Salerno, 23-24 novembre 2012; reperibile *on line* *http://www.associazionedeicostituzionalisti.it/sites/default/files/bandigare/Relazione%20Caretti.pdf.*