NOMOS
Le attualità nel diritto
Quadrimestrale di Teoria generale,
Diritto pubblico comparato e Storia costituzionale

FLAVIA ZORZI GIUSTINIANI*

LA POSIZIONE COMUNE DELL'UNIONE AFRICANA SULL'APPLICAZIONE DEL DIRITTO INTERNAZIONALE AL CYBERSPAZIO E LA DECISIONE DI ADEGUATEZZA UE DELLA NUOVA NORMATIVA SVIZZERA IN MATERIA DI PROTEZIONE DEI DATI**

SOMMARIO: 1. La Posizione comune dell'Unione africana sull'applicazione del diritto internazionale al cyberspazio. 2. L'Unione europea conferma l'adeguatezza della nuova normativa svizzera in materia di protezione dei dati.

1. La Posizione comune dell'Unione africana sull'applicazione del diritto internazionale al cyberspazio

Nel semestre in rassegna una prima novità di rilievo si deve all'Unione africana (UA), il cui *Peace and Security Council* (PSC) il **29 gennaio** scorso, durante la sua 1196esima seduta, ha adottato la "Common African Position on the Application of International Law to the Use of Information and Communication Technologies in Cyberspace". Lo stesso documento è stato poi approvato dall'Assemblea dell'UA il **18 febbraio**. Il risultato è giunto, non a caso, dopo l'ondata di attacchi cibernetici che nel 2023 ha investito il continente africano, e in particolare i sistemi informatici della Commissione dell'UA e del governo keniota come pure l'infrastruttura elettorale nigeriana. Benché infatti la cybersicurezza fosse uno dei progetti bandiera dell'Agenda 2063[1] dell'UA sin dal suo lancio nel 2013, negli anni più recenti gli Stati membri non gli avevano assegnato la dovuta priorità. Il rilievo del documento, che è stato adottato all'unanimità, è particolarmente significativo giacché esprime la posizione in materia di ben cinquantacinque Stati diversi, quanti sono i membri dell'UA. Della Common African Position (CAP) è interessante anche

* Professoressa associata di Diritto dell'Unione europea – Università degli Studi Link, Roma.
** Contributo sottoposto a *peer review*.
[1] L'Agenda 2063 è stata sottoscritta nel maggio del 2013, durante il Giubileo d'Oro per il 50° anniversario della Fondazione dell'Unione Africana, dai capi di Stato e di governo di tutti i Paesi africani come affermazione del loro impegno per l'Africa del futuro.

ISSN 2279-7238

il processo che ha portato alla sua adozione, trattandosi di un *lawmaking process* che si è svolto in varie fasi e ha coinvolto una molteplicità di *stakeholders*.

In particolare, il *lawmaking process* è stato condotto da due organi dell'UA, il PSC e la Commissione sul diritto internazionale, mentre vi hanno partecipato, tra gli altri, funzionari degli altri organi competenti in aree correlate al cyberspazio, come pure vari autorevoli giuristi quali Dire Tladi, Makane Mbengue, Erika de Wet, Mamadou Hébié e Martha Bradley. La prima fase del processo, dedicata al *capacity-building*, ha ospitato al suo interno un vero e proprio programma di formazione per diplomatici, esperti e giuristi governativi africani, che è stato condotto da esperti del settore del calibro di Michael Schmitt, Liis Vihul, Dapo Akande e Marko Milanovic[2]. Nella seconda fase si è poi svolta la redazione vera e propria del testo, che è stato presentato in prima battuta dallo *Special Rapporteur* Mohamed Helal e approvato in prima lettura all'unanimità dalla Commissione sul diritto internazionale nel maggio 2023. Il testo è stato di seguito sottoposto, su richiesta del PSC, a vari *stakeholders*, tra cui in particolare funzionari di organizzazioni internazionali quali l'Organizzione degli Stati Americani e il Comitato internazionale di Croce Rossa, e molteplici esperti africani e non. Sulla scorta dei *feedback* ricevuti, lo *Special Rapporteur* ha presentato una seconda versione, e successivamente il PSC ha deciso di istituire un gruppo di lavoro incaricato di redigere la versione finale del testo. Detto gruppo di lavoro, va rilevato, è stato composto da delegazioni nazionali molto ampie e variegate, composte tra l'altro da diplomatici, avvocati, funzionali militari e dell'intelligence, ingegneri, esperti di *cybersecurity* e accademici. Come correttamente evidenziato dalla *Special Rapporteur*, le modalità di svolgimento del *lawmaking process* e la varietà come pure l'impegno degli *stakeholders* e degli esperti coinvolti hanno facilitato notevolmento la negoziazione e redazione del CAP, e hanno altresí contribuito ad aumentarne la legittimità[3].

La CAP è strutturata in undici sezioni, un preambolo e una conclusione. Ogni sezione, ad eccezione di quella relativa al *capacity building*, esordisce riportando le regole di base del rispettivo ambito di diritto internazionale, per poi discuterne l'applicabilità nel cyberspazio. Di seguito si riportano le posizioni assunte in relazione alle tematiche più controverse, ovvero la sovranità, il non intervento e l'uso della forza nel cyberspazio.

In tema di sovranità, anzitutto, il CAP afferma *in primis* che il principio di sovranità territoriale è una norma primaria del diritto internazionale, e che in quanto tale si applica anche alla condotta degli Stati nel cyberspazio[4]. Adotta poi quello che è stato definito come un approccio "puro" alla sovranità cibernetica[5], secondo il quale "any unauthorized access by a State into the ICT infrastructure located on the territory of a foreign State is unlawful"[6].

---

[2] I primi tre sono i curatori del Manuale di Tallinn sul diritto internazionale applicabile alla *cyberwarfare*, mentre Milanovic é cofondatore dell'"Oxford Process on International Law Protections in Cyberspace".

[3] Cfr. M. HELAL, *The Common African Position on the Application of International Law in Cyberspace: Reflections on a Collaborative Lawmaking Process*, in *EJIL Talk*, 5 febbraio 2024, on-line.

[4] Cfr. par. 13 del CAP.

[5] In merito al quale si rinvia a K.J. HELLER, *In defense of pure sovereignty in cyberspace*, in *International Law Studies*, n. 97/2021, 1433 ss.

[6] Cfr. par. 16 del CAP.

Di conseguenza rigetta pure l'ammissibilità della soglia *de minimis*, che sembra invece accolta dal Manuale Tallin, stabilendo quanto segue: "the obligation to respect the territorial sovereignty of States, as it applies in cyberspace, does not include a *de minimis* threshold of harmful effects below which an unauthorized access by a State into the ICT infrastructure located on the territory of a foreign State would not be unlawful"[7]. Specifica poi ulteriormente che il suddetto principio di sovranità territoriale impedisce agli Stati di esercitare la loro "enforcement authority on the territory of a foreign State (…) even if the exercise of such enforcement authority by a State does not have harmful effects, whether virtual or physical, on the territory of a foreign State"[8].

Quanto al principio del non intervento, secondo il CAP "in the internal and external affairs of States (it) is a principle of general international law"[9] e si applica nel cyberspazio[10]. Rilevante è poi l'interpretazione ampia che viene accolta di detto principio. La coercizione che sarebbe proibita dal dominio riservato, secondo il documento, va intesa "as a policy that is designed to impose restraints on the will of a foreign State"[11], non essendo necessario che si estrinsechi in una condotta della Stato che assurge "to the level of completely depriving a foreign State of its freedom of choice or to compel that State to either act or refrain from acting involuntarily"[12].

Infine, in merito all'uso della forza, dopo aver riconosciuto l'applicabilità al cyberspazio delle norme della Carta Onu e consuetudinarie che regolano il suddetto uso, stabilisce quanto segue: "a cyber operation that destroys, inflicts damage, or *permanently disables critical infrastructure or civilian objects* within a State, may be considered as amounting to a use of force under international law. Similarly, a cyber operation that targets a military asset by destroying, damaging, or deactivating a missile defense system, could constitute a violation of the prohibition on the use of force"[13]. Quanto alla legittima difesa, dopo aver accolto la tesi tradizionale che limita il suo ricorso al caso di risposta ad un attacco armato, con riguardo alla questione della risposta agli attacchi imminenti non adotta una posizione definitiva, ritenendo che la questione "requires further study and deliberation between States taking into consideration both the unique characteristics of cyberspace and cyber-operations and the implications that any rules that may emerge in relation to this question may have for the integrity of the prohibitions on the threat or use of force"[14]. Infine, riguardo all'uso della forza in autodifesa contro attori non statali, il CAP la ritiene lecita "only if their acts are attributed to a State according to the law of State responsibility"[15].

[7] *Ibid.*.
[8] Cfr. par. 15 del CAP.
[9] Cfr. par. 26 del CAP.
[10] Cfr. par. 29 del CAP.
[11] Cfr. par. 31 del CAP.
[12] Cfr. par. 32 del CAP.
[13] Cfr. par. 40 del CAP, corsivo nostro.
[14] Cfr. par. 42 del CAP.
[15] Cfr. par. 43 del CAP.

2. L'Unione europea conferma l'adeguatezza della nuova normativa svizzera in materia di protezione dei dati

Un altro sviluppo importante è poi costituito dalla decisione positiva della Commissione europea in merito all'adeguatezza del livello di protezione dei dati garantito dalla normativa svizzera in materia, ovvero dalla nuova legge svizzera sulla protezione dei dati (nLPD), entrata in vigore il 1° settembre 2023. La suddetta determinazione, che è richiesta dal il Regolamento europeo sulla protezione dei dati (GDPR), è contenuta nel rapporto sull'adeguatezza del livello di protezione dei dati in diversi Paesi terzi, pubblicato dalla Commissione il 15 gennaio scorso, e fa seguito all'entrata in vigore della nLPD. Ne discende che i dati personali possono continuare a essere trasferiti da un Paese dell'Unione alla Confederazione svizzera senza la necessità di ulteriori garanzie oltre a quelle offerte dalla nLPD. Vediamole nel dettaglio.

La nLPD costituisce una revisione totale della prima legge federale sulla protezione dei dati, risalente al 1992 e già oggetto di due revisioni parziali nel 2009 e nel 2019. Il nuovo strumento trova per l'appunto la sua ragion d'essere non soltanto nell'esigenza di assicurare, alla popolazione svizzera una protezione dei propri dati adeguata e aggiornata alle ultime evoluzioni tecnologiche e sociali, ma anche di garantire la compatibilità del diritto nazionale con il diritto dell'Unione europea, nella specie con il GDPR. La compatibilità con il GDPR, in particolare, è funzionale ad assicurare una continua libera circolazione dei dati con la Ue e, in ultima analisi, ad evitare una perdita di competitività delle imprese svizzere.

Le novità principali introdotte dalla rinnovata nLPD sono le seguenti. Anzitutto, cambiamenti rilevanti attengono all'ambito di applicazione della normativa. Da un punto di vista oggettivo, la nLPD riguarda esclusivamente i dati delle persone fisiche, ad eccezione quindi delle persone giuridiche. Più in particolare, la categoria dei dati considerati sensibili ora include anche dati genetici e biometrici. Inoltre, *ratione loci*, il campo di applicazione è ampliato, sulle orme del GDPR. L'art. 3 stabilisce che la nLPD "si applica alle fattispecie che generano effetti in Svizzera, anche se si verificano all'estero". L'ampiezza della norma è invero maggiore dell'analoga disposizione del GDPR, benché i suoi esatti confini restino in parte indefiniti. Non è chiaro infatti se gli effetti a cui si riferisce l'art. 3 siano gli effetti giuridici o gli effetti fattuali.

Si prevede, poi, che le imprese straniere che trattano dati personali relativi a persone in Svizzera, a certe condizioni (quali la presenza di un rischio elevato per i diritti dei soggetti interessati), debbano obbligatoriamente designare un rappresentante in Svizzera il quale, al pari del rappresentate UE previsto dal GDPR, sarà l'interlocutore per i singoli interessati e per l'autorità svizzera per il trattamento dei dati personali (ovvero l'Incaricato Federale della Protezione dei Dati e della Trasparenza (IFPDT)).

Dal GDPR vengono mutuati i concetti di "Privacy by Design" (protezione dei dati sin dalla concezione) e "Privacy by Default" (protezione dei dati per impostazione predefinita). Il primo principio implica che gli sviluppatori integrino la protezione e il rispetto della vita privata degli utenti nella struttura stessa del prodotto o del servizio tramite il quale si

raccolgono i dati personali. La *privacy by default*, invece, garantisce il livello di sicurezza più elevato dalla messa in circolazione del prodotto o del servizio, attivando in modo automatico, senza un necessario intervento da parte dell'utente, tutte le misure atte alla protezione dei dati e alla limitazione del loro utilizzo. In altri termini, tutti i *software*, il materiale e i servizi informatici devono essere configurati in modo da garantire la protezione dei dati e il rispetto della vita privata degli utenti.

Si introduce poi l'obbligo, per i titolari del trattamento, di effettuare una preventiva valutazione d'impatto sulla protezione dei dati qualora il trattamento possa comportare un rischio elevato per la personalità o i diritti fondamentali della persona interessata, salve alcune ipotesi di esenzione (ad esempio, se il titolare è tenuto a effettuare il trattamento in virtù di un obbligo legale). Nel caso in cui il rischio, nonostante la valutazione di impatto, rimanga elevato, il titolare del trattamento dovrà consultare l'IFPDT.

Ancora, si introduce nella legge la nozione di profilazione, ossia il trattamento automatizzato dei dati personali, come pure l'obbligo, per i titolari e i responsabili del trattamento, di tenere un registro delle rispettive attività di trattamento dei dati, ferma la possibilità di eccezioni per imprese con meno di 250 collaboratori i cui trattamenti comportino rischi ridotti. Oltre a ciò, la raccolta di qualsiasi tipo di dati personali – e non più soltanto di quelli detti sensibili – deve portare all'informazione preventiva delle persona interessate.

Infine, sul piano dell'*enforcement*, rispetto al pregresso le possibili sanzioni sono ben più elevate, mentre all'IFPDT sono stati conferiti maggiori poteri di vigilanza. Nella nuova LPD, i trasgressori sono puniti con un sistema di sanzioni penali con multe fino a 250'000 franchi svizzeri.