Raccomandazione 5G della Commissione europea

Proposte riguardo ai Fattori di Rischio e agli Strumenti di Gestione

1. La Raccomandazione 5G e la Proposta di Azione agli Stati Membri

La Raccomandazione della Commissione europea del 26 marzo 2019 riguardante la cybersicurezza delle reti 5G (la "**Raccomandazione 5G**") dà istruzioni agli Stati Membri circa l'adozione di un approccio concertato alla sicurezza nel 5G. Entro il 30 giugno 2019 gli Stati Membri dovranno **effettuare una valutazione dei rischi delle reti 5G**. Agli Stati Membri viene poi chiesto di creare e concordare entro il 31 dicembre 2019 una c.d. "toolbox" (insieme di strumenti), che dovrebbe includere:

- Un inventario dei rischi di sicurezza per le reti 5G, che copra due distinte categorie di rischio: (i) fattori tecnici e (ii) "altri" fattori; e,

- Una serie di proposte di misure di attenuazione di tali rischi.

La presente analisi si concentra sulla categoria dei rischi indotti da "altri" fattori e propone specifici criteri in base ai quali tali rischi dovrebbero essere valutati (paragrafo 2). Proponiamo quindi un modello indicativo di base per valutare i rischi indotti da "altri" fattori.

L'analisi evidenzia inoltre alcuni aspetti legali rilevanti ai fini di un'applicazione efficace delle misure di attenuazione del rischio da parte degli Stati Membri (paragrafo 3).

2. Criteri di base per valutare gli "altri" fattori di rischio

2.1 Importanza della distinzione tra "altri" fattori 'introdotti' e fattori tecnici

La Raccomandazione 5G effettua una chiara distinzione tra fattori tecnici e "*altri*" fattori. Una distinzione simile viene spesso fatta nel settore dell'*information and communication technology* ("**ICT**"), in cui i rischi tecnici possono essere paragonati alle "vulnerabilità intrinseche" di un prodotto. Queste includono i difetti di qualità o le carenze accidentali di un software, servizio o hardware ICT. Affrontare tali rischi non è generalmente problematico, dal momento che gli interessi del fornitore e del compratore – fornire/acquistare hardware o software funzionanti e sicuri - sono allineati.

La categoria degli "altri" fattori riguarda invece fattori esterni, e include anche le c.d. "vulnerabilità introdotte", che si riferiscono ad una manipolazione intenzionale o

accidentale dell'hardware, software o servizio del fornitore. In materia di sicurezza ICT, si ritiene solitamente che le *vulnerabilità introdotte* traggano origine da moventi illeciti e occulti di terzi.[1]

La Raccomandazione 5G elenca una serie di aspetti da tenere in considerazione nella categoria degli "altri" fattori:

> "…tra l'altro, del rischio generale di influenza da parte di un paese terzo, in particolare in relazione al suo modello di governance, all'assenza di accordi di cooperazione sulla sicurezza o di disposizioni analoghe, quali le decisioni di adeguatezza … se tale paese sia parte di accordi multilaterali, internazionali o bilaterali in materia di cybersicurezza, lotta alla criminalità informatica o protezione dei dati."[2]

I seguenti sotto-paragrafi elencano alcuni fattori che potrebbero essere inclusi in un inventario dei rischi da "altri" fattori.

2.2 Mancanza di trasparenza

Una valutazione dei rischi della sicurezza 5G richiederà necessariamente informazioni e cooperazione da parte dei fornitori di servizi, software e componenti 5G (i "Fornitori") per quanto concerne sia i fattori tecnici sia gli "altri" fattori. Poiché la sicurezza 5G attiene alla sicurezza nazionale, l'onere della prova a fondamento di una qualunque pretesa o azione dovrebbe essere a carico del Fornitore. Il fatto stesso che un Fornitore non sia in grado di garantire trasparenza o di cooperare quando gli viene richiesto di fornire informazioni dovrebbe essere considerato di per sé solo un fattore di rischio.[3]

---

[1] Si veda il documento NCSC "A Framework for Assessing Risk": https://www.dni.gov/files/NCSC/documents/products/SCRM_Framework_for_Assessing_Risk_White_Paper.pdf; si vedano anche le pagine da 4 a 7 del documento "Investigative Report on the U.S. National Security Issues Posed by Chinese Telecommunications Companies Huawei and ZTE", U.S. House of Representatives, Congresso n. 112, 8 ottobre 2012". Disponibile su: https://intelligence.house.gov/sites/intelligence.house.gov/files/documents/huawei-zte%20investigative%20report%20(final).pdf. Si veda anche il paragrafo 8 del documento "Analysis of vulnerability to espionage", da parte del Servizio olandese di Intelligence Generale e Sicurezza (AIVD), Direttorato Generale per la Sicurezza (DGV), Ministero dell'interno e delle relazioni con il Regno: https://fas.org/irp/world/netherlands/aivd-vuln.pdf.

[2] Raccomandazione 5G, p. 4.

[3] Si raffrontino i requisiti di export control per l'informativa sull'utilizzatore finale, si veda "The Wassenaar Arrangement Participating States' non-exhaustive List of Advisory Questions for Industry", https://www.wassenaar.org/app/uploads/2018/12/Advisory-Questions-for-Industry-Amended.pdf. Si raffronti anche la proposta di legge francese nel *code des postes et des communications électroniques* in

I requisiti di trasparenza dovrebbero includere, ad esempio:

1. Condividere informazioni sulla proprietà, il controllo e le fonti di finanziamento del Fornitore e/o dei sub-fornitori, e in particolare qualora la proprietà, il controllo o le fonti di finanziamento siano collegati o riferibili a uno Stato estero.[4]

2. Accordi di *Intelligence sharing* tra i Fornitori e i sub-fornitori.[5]

3. Fornire informazioni sulle normative che impongano al Fornitore e ai sub-fornitori di rivelare informazioni a Stati esteri.

2.3 Dipendenza da Stati esteri – rischio di influenza

Un focus primario nell'inventario degli "altri" fattori dovrebbe essere dato dall'identificazione dei legami o grado di dipendenza tra un particolare fornitore e uno Stato estero. Tali legami di dipendenza potrebbero influenzare l'autonomia e la capacità decisionale del Fornitore, nonché influenzare o spingere il Fornitore ad adottare decisioni operative o di business in relazione ai clienti della rete 5G che non siano basate in primo luogo sulla logica strategica ed economica propria del Fornitore, ma che siano invece guidate dalle politiche estere o di sicurezza di uno Stato straniero.

L'indicatore di dipendenza può essere suddiviso in quattro sottocategorie:

1. **Proprietà diretta o indiretta da parte di uno Stato**: se un Fornitore è di proprietà di uno Stato estero, quello Stato controllerà di fatto il Fornitore, determinando un evidente rischio di influenza. In ogni caso, **dovrebbe essere tenuta in considerazione anche la proprietà parziale e indiretta** da parte di uno Stato. Tali valutazioni dovrebbero essere allineate con quanto previsto dal nuovo quadro dell'Unione europea relativo al controllo degli investimenti diretti stranieri ("**IDS**").[6]

---

cui gli operatori sono responsabili per la propria richiesta di autorizzazione, http://www.assemblee-nationale.fr/15/propositions/pion1722.asp.

[4] Si veda "Supply Chain Vulnerabilities from China in the U.S. Federal Information and Communication Technology", https://docs.house.gov/meetings/IF/IF16/20180516/108301/HHRG-115-IF16-20180516-SD105-U105.pdf, p. 13, in cui si afferma che "*Ai fini del SCRM [Gestione del Rischio della Filiera di Fornitura] sono importanti anche i legami finanziari con entità sospette, incluse imprese possedute o sostanzialmente controllate dallo Stato, in quanto indicativi di potenziali vettori di influenza nefasta*."

[5] *Id.* p. 16, che analizza i *corporate intelligence-sharing agreements*: "*Partnership commerciali che condividono dati di applicazione di programma, informazioni di configurazione o anche policies di diffusione, potrebbero però inavvertitamente fornire a soggetti maliziosi le informazioni di cui necessitino per infiltrarsi nei sistemi federali di ICT*".

[6] Si vedano l'articolo 4.2 a e la premessa 13 del nuovo Regolamento (UE) 2019/452 del Parlamento europeo e del Consiglio del 19 marzo 2019 che stabilisce un quadro per il controllo degli investimenti diretti stranieri all'interno dell'Unione (il "**Quadro di Controllo IDS dell'UE**"). Si segnala che l'Italia si è già

2. **Controllo**: Anche nel caso in cui uno Stato estero non ne detenga direttamente o indirettamente la proprietà, lo stesso potrebbe avere la capacità di controllare un Fornitore attraverso le strutture di governance o il contesto normativo della giurisdizione in cui in Fornitore ha la propria sede. Le Migliori Pratiche dell'Unione europea in materia di misure restrittive potrebbe fornire una guida adeguata per la determinazione del livello di controllo.[7]

3. **Influenza finanziaria**: un Fornitore che riceve fondi statali o garantiti da uno Stato potrebbe essere soggetto ad influenza da parte di quello Stato. Questo fattore è anche specificamente citato nel Quadro di Controllo IDS dell'UE come un importante fattore da tenere in considerazione.[8]

4. **Influenza politica**: un Fornitore potrebbe avere altri legami con uno Stato estero, ad esempio laddove gli venga legalmente o formalmente imposta la presenza di una rappresentanza politica all'interno del suo organo amministrativo o di gestione.[9] Un esempio potrebbe essere il caso in cui un Fornitore abbia volontariamente modificato il proprio statuto nel senso di prevedere la consultazione di comitati politici prima di adottare decisioni rilevanti.[10]

---

da tempo dotata di una propria normativa sul controllo degli investimenti, anche non esteri, nei settori della difesa e della sicurezza nazionale, nonché dell'energia, dei trasporti e delle comunicazioni (D.L. 21/2012). Tale normativa ha introdotto poteri speciali, esercitabili dal governo, di imposizione di specifiche condizioni e di veto rispetto ad operazioni societarie nei settori in questione nonché (modifica recentissima: si veda l'art. 1 del disegno di legge di conversione del decreto legge n. 22 del 2019 sulla cosiddetta *Hard Brexit*, approvato dal Senato il 23 aprile 2019 e quindi passato all'esame della Camera dei Deputati) proprio rispetto ai contratti per l'acquisto di beni o servizi relativi alla progettazione, alla realizzazione, alla manutenzione e alla gestione delle reti inerenti i servizi di comunicazione elettronica a banda larga basati sulla tecnologia 5G, qualora gli stessi contratti siano posti in essere con soggetti esterni all'Unione europea. Link: https://www.normattiva.it/urires/N2Ls?urn:nir:stato:decreto.legge:2012-03-15;21!vig=; http://www.camera.it/temiap/documentazione/temi/pdf/1155963.pdf?_1556191521255.

[7] Si vedano le Migliori Pratiche disponibili sul sito del Consiglio dell'Unione europea: https://data.consilium.europa.eu/doc/document/ST-8519-2018-INIT/en/pdf.

[8] Si veda nota 6 e, per esempio, un caso di influenza statale sul settore finanziario in Cina, punti 2.5 – 2.8 del documento WTO "China's Trade-Disruptive Economic Model, Communication from the United States" WT/GC/W/745, del 16 luglio 2018.

[9] *Id.* paragrafo B. Si veda anche la pubblicazione di Global Times 2016/12/18 21:53:39 http://www.globaltimes.cn/content/1024360.shtml.

[10] In base agli articoli elencati qui sotto, risulta che un numero elevato di società cinesi quotate abbia modificato il proprio statuto per fare in modo che i comitati di partito siano consultati prima di assumere decisioni importanti: https://asia.nikkei.com/Politics/Chinese-enterprises-write-Communist-Party-s-role-into-charters, https://asia.nikkei.com/Politics/Chinese-corporate-sector-falls-further-under-party-s-sway, si vedano anche i reports dell'UE e della Camera di Commercio tedesca in cui si esprime preoccupazione circa il fatto che JV di proprietà estera che operano in Cina siano state spinte a costituire organizzazioni di partito

2.4 Norme di conflitto di Stati esteri

La Raccomandazione 5G elenca espressamente i modelli di governance estera, il che include naturalmente i regimi giuridici cui è soggetto un Fornitore. Quindi, la giurisdizione del luogo in cui si trovano il quartiere generale o la società capogruppo del Fornitore è estremamente rilevante, dal momento che la capogruppo del Fornitore è per legge assoggettata a tali normative. In aggiunta, a qualunque società controllata dalla capogruppo, ad esempio un Fornitore stabilito nella UE, potrebbe essere richiesto di adeguarsi a tali disposizioni, *ex lege* o attraverso l'applicazione extraterritoriale delle stesse. Vi è di conseguenza il rischio che, se la società capogruppo è tenuta a conformarsi a determinate previsioni di legge, essa dia istruzioni anche alle proprie controllate estere di allinearsi alle stesse.[11]

È fondamentale verificare se le previsioni di tali regimi giuridici stranieri siano o possano venire in conflitto con leggi o interessi di sicurezza fondamentali dell'UE o degli Stati Membri.

Qui di seguito tre esempi di casi in cui un Fornitore 5G potrebbe trovarsi ad affrontare una situazione in cui la normativa UE è in conflitto con quella straniera.

1. Per la normativa dell'Unione europea, la riservatezza delle comunicazioni (incluse quelle societarie) è un diritto fondamentale.[12] Le restrizioni a tale diritto sono consentite solamente in circostanze molto limitate e rigorosamente definite.

2. Le regole UE sulla privacy dei dati previste nel General Data Protection Regulation ("GDPR").

3. I regimi giuridici che potrebbero trovare applicazione in relazione alla raccolta di informazioni da parte di uno Stato. Ad esempio, la "Chinese National Intelligence

---

al proprio interno, dando così al partito un ruolo di governance e decisionale in questioni rilevanti per le JV: http://www.europeanchamber.com.cn/en/press-releases/2583/chamber_stance_on_the_governance_of_joint_ventures_and_the_role_of_party_organisations, http://china.ahk.de/news/single-view/artikel/press-statement-increasing-business-challenges-delegations-of-german-industry-commerce-in-china-concerned-about-growing-influence-of-chinese-co/?no_cache=1.

[11] Per fare un paragone, le sanzioni US e UE sono spesso estese, direttamente o indirettamente (attraverso policy societarie), alle controllate che si trovano al di fuori di US o UE.

[12] Si veda C-450/06 Varec SA, ECLI:EU:C:2008:91. Si veda anche la Carta dei Diritti Fondamentali dell'Unione europea e la Direttiva 2002/58/CE.

Law" ("**NIL**") [13] stabilisce a carico delle organizzazioni e dei cittadini cinesi ampi obblighi di cooperazione con le autorità cinesi, quando richiesto, riguardo alla raccolta di informazioni. Tali obblighi potrebbero estendersi di fatto, in via extraterritoriale, alle controllate, incluse ad esempio quelle europee, di società capogruppo cinesi.[14]

2.5 Regime giuridico dello Stato d'origine di un Fornitore: *rule of law* e separazione dei poteri nel regime giuridico straniero

Nell'analizzare la normativa degli Stati esteri e il suo impatto sui Fornitori, è altrettanto importante prendere in considerazione il modello generale di governance dello Stato estero rispetto ai suoi cittadini e società. In particolare, l'analisi dovrebbe concentrarsi sullo stato del sistema giudiziario, sul rispetto del principio dello Stato di diritto e sull'esistenza o meno di un'adeguata separazione dei poteri.

La *rule of law* è un principio fondamentale sancito dall'Articolo 2 del Trattato dell'Unione europea.[15] Esso include il principio di legalità, che implica un processo di emanazione delle leggi trasparente, responsabile, democratico e pluralistico; la certezza legale; il divieto di arbitrarietà dei poteri esecutivi; tribunali indipendenti e imparziali; un'efficace revisione giudiziaria basata sul rispetto dei diritti fondamentali; e l'uguaglianza di fronte alla legge.[16] È importante distinguere e comprendere la differenza tra *rule of law* e *rule by law*. Per esempio, la Cina ha introdotto il concetto di

[13] Un fattore di rischio insito nella costruzione di una legge come la NIL è la possibile applicazione extraterritoriale. Non vi sono limiti geografici espliciti nella NIL. Pertanto il concetto di organizzazione potrebbe potenzialmente riferirsi ad un intero gruppo, includendovi sia la capogruppo sia le controllate estere. In aggiunta, poiché la NIL si applica ai cittadini cinesi, vi è un controllo effettivo anche su di una controllata europea nel caso in cui il suo management sia composto da cittadini cinesi (i quali avranno probabilmente un separato obbligo legale di adeguarsi alla NIL). Una capogruppo potrebbe anche semplicemente decidere di sostituire il management o le funzioni chiave all'interno di una società europea con cittadini cinesi per ottenere efficacemente tale applicazione extraterritoriale di fatto. Si veda anche un'introduzione generale del "Draft National Intelligence law in China", del giugno 2018, disponibile su: https://www.canada.ca/en/security-intelligence-service/corporate/publications/china-and-the-age-of-strategic-rivalry/chinas-intelligence-law-and-the-countrys-future-intelligence-competitions.html

[14] Si veda la traduzione in inglese della "Chinese National Intelligence law", in particolare l'articolo 7, disponibile su: http://en.pkulaw.cn/display.aspx?cgid=313975&lib=law

[15] L'Articolo 2 recita: "L'Unione si fonda sui valori del rispetto della dignità umana, della libertà, della democrazia, dell'uguaglianza, dello Stato di diritto e del rispetto dei diritti umani, compresi i diritti delle persone appartenenti a minoranze. Questi valori sono comuni agli Stati Membri in una società caratterizzata dal pluralismo, dalla non discriminazione, dalla tolleranza, dalla giustizia, dalla solidarietà e dalla parità tra donne e uomini."

[16] Si vedano le spiegazioni fornite nel Briefing dei Parlamenti europei del 2016, "Understanding the EU Rule of Law" disponibile su http://www.europarl.europa.eu/EPRS/EPRS-Briefing-573922-Understanding-EU-rule-of-law-mechanisms-FINAL.pdf

rule by law al fine di legalizzare e istituzionalizzare la leadership del partito. Ad ogni modo, la leadership cinese non sembra intenzionata a copiare il "costituzionalismo occidentale', la 'separazione dei poteri,' o l''indipendenza giudiziaria.'"[17]

L'esame del modello di governance di uno Stato estero è quindi essenziale per valutare se un Fornitore di servizi, software o hardware 5G nell'UE, che possa essere esposto a una legge straniera, abbia mezzi efficaci per opporsi legalmente a richieste provenienti, per esempio, da un'autorità estera di intelligence dello Stato della capogruppo, per il supporto in un'intercettazione che è illegale nell'UE o contraria alla sicurezza di uno Stato membro dell'UE.

Molti Stati hanno leggi di *intelligence* attraverso cui le autorità possono richiedere la cooperazione da parte degli operatori per il supporto nella raccolta di informazioni estere. In ogni caso, in paesi con una forte tradizione di Stato di diritto e separazione dei poteri, l'ambito di applicazione della legge sarà di norma chiaramente definito e assegnerà una forte protezione ai diritti fondamentali. Le richieste di supporto agli operatori saranno di conseguenza adottate, con più probabilità, da un'autorità indipendente e spesso giudiziaria, che ha poteri separati dal governo o dal partito di potere.

Per valutare se uno Stato estero offra protezione giudiziaria ai soggetti privati per opporsi all'influenza di uno Stato, può essere esaminata la combinazione dei seguenti parametri:

1. Se le direttive o leggi locali abbiano una finalità chiara e ben circoscritta, come ad esempio la minaccia alla sicurezza nazionale (es. terrorismo), con la conseguenza che non vi si potrebbe fare affidamento per richiedere agli operatori di effettuare intercettazioni di comunicazioni in genere;

2. Se l'ordinamento abbia una funzione di controllo giudiziario indipendente, ossia che le decisioni sulle intercettazioni di comunicazioni siano adottate da autorità giudiziarie indipendenti (ad esempio l'autorità giudiziaria); e

3. l'ordinamento sia basato sulla netta separazione dei poteri, che assicuri l'indipendenza del giudiziario rispetto ai partiti o alle autorità di governo che abbiano richiesto la decisione.

[17] Si veda un articolo da Diplomat, che cita a sua volta un articolo da parte del presidente cinese; disponibile su https://thediplomat.com/2019/02/xi-china-must-never-adopt-constitutionalism-separation-of-powers-or-judicial-independence/. Si vedano ulteriori spiegazioni e fonti su: https://sinopsis.cz/en/lawfare-by-proxy-huawei-touts-independent-legal-advice-by-a-ccp-member/.

Due esempi di come queste componenti lavorino assieme si riscontrano in alcuni casi provenienti dagli USA e dal Canada.[18]

3. Misure/metodi di gestione del rischio

La Raccomandazione 5G dà istruzioni agli Stati Membri di predisporre "misure di gestione dei rischi" adeguate, efficaci e proporzionate al fine di attenuare i rischi di cybersicurezza individuati a livello nazionale e unionale.[19] Questo paragrafo tratta una serie di aspetti giuridici che gli Stati Membri dovrebbero affrontare per garantire che qualunque misura di gestione del rischio sia giuridicamente fondata e applicabile.

3.1 Base giuridica per l'adozione di misure da parte degli Stati Membri

Una pre-condizione dell'applicazione di misure di gestione del rischio è che gli Stati Membri dispongano di una base giuridica per implementarle.

Come primo passo, gli Stati Membri dovrebbero assicurarsi di avere dato esecuzione alle due direttive specificamente richiamate nella Raccomandazione[20], per far sì che le proprie autorità nazionali possano (i) imporre requisiti di sicurezza agli operatori della rete e, se necessario, emettere disposizioni vincolanti nei loro confronti, e (ii) quando concedono le autorizzazioni generali per le comunicazioni elettroniche, integrarle con condizioni volte a tutelare la sicurezza della rete contro accessi non autorizzati.[21]

---

[18] Il caso US (*United States v. Microsoft Corp*.) del 2017 riguardava il fatto se Microsoft fosse obbligata a fornire alle autorità US i dati immagazzinati in Irlanda in forza di un mandato. La corte d'appello si è pronunciata in favore di Microsoft e ha annullato il mandato. Link a United States v. Microsoft Corp: https://www.bloomberg.com/news/articles/2019-02-24/huawei-frightens-europe-s-data-protectors-america-does-too, e https://www.reuters.com/article/us-microsoft-usa-warrant/microsoft-wins-landmark-appeal-over-seizure-of-foreign-emails-idUSKCN0ZU1RJ. La sostanza del caso canadese è simile a quella del caso US. Il Giudice di una corte federale ha stabilito, nel luglio 2018, che la competenza dell'intelligence canadese è strettamente limitata al territorio domestico, a meno che non sia in questione la sicurezza nazionale. Di conseguenza, il Giudice indipendente ha impedito efficacemente un'estensione dell'ambito di applicazione della legge, pronuncia resa possibile attraverso la procedura di approvazione e la separazione dei poteri. Link al caso candese: https://www.theglobeandmail.com/canada/article-judge-limits-canadas-international-spying-reach/.

[19] Voce 14 della Raccomandazione.

[20] La Voce 4 della Raccomandazione fa riferimento alla Direttiva 2002/21/EC e alla Direttiva 2002/20.

[21] Articoli 13a e 13b della Direttiva 2002/21/EC e, *inter alia*, Annex, voce 16 della Direttiva 2002/20. In Italia, per esempio, il Disciplinare di Gara pubblicato nel 2018 dal Ministero dello Sviluppo Economico per l'assegnazione di diritti d'uso delle frequenze radio nel 5G prevede espressamente l'obbligo in capo agli aggiudicatari di garantire la sicurezza delle reti pubbliche contro l'accesso non autorizzato, conformemente alla normativa nazionale e dell'Unione europea. Si veda art. 10.6. Link: https://www.mise.gov.it/images/stories/normativa/Disciplinare_Gara_multibanda2018.pdf

3.2 Esempio di applicazione nazionale efficace

La Raccomandazione 5G propone che le misure includano "processi volti a garantire l'esistenza e l'applicazione del controllo degli accessi" e che "identifichino prodotti, servizi o fornitori considerati potenzialmente non sicuri etc."[22]

Gli Stati Membri dovrebbero assicurare che le proprie normative nazionali consentano l'adozione di misure efficaci di attenuazione del rischio. In Francia, ad esempio, il Primo Ministro emette uno specifico ordine (Fr: *arrêté*) che elenca le componenti e gli apparecchi tecnici soggetti ad una valutazione del rischio prima di poter essere immessi nel mercato francese.[23] Inoltre è stata avanzata una nuova proposta di legge che prevede una procedura simile, ma dedicata specificamente al 5G.[24] La violazione di queste previsioni di legge può comportare sanzioni.[25] L'Italia, in recepimento della Direttiva (UE) 2016/1148 (c.d. Direttiva NIS), intesa a definire le misure necessarie a conseguire un elevato livello di sicurezza delle reti e dei sistemi informativi, ha adottato una legge, in via di progressiva attuazione, che si applica agli operatori di servizi essenziali, tra cui le infrastrutture digitali, e ai fornitori di servizi digitali, i quali sono chiamati ad adottare misure tecniche e organizzative adeguate e proporzionate alla gestione dei rischi e a prevenire e minimizzare l'impatto degli incidenti a carico della sicurezza delle reti e dei sistemi informativi[26].

3.3 Raccomandazioni aggiuntive per leggi e procedure nazionali

Gli Stati Membri dovrebbero prendere in considerazione quanto segue:

1. Centralizzare la responsabilità per la valutazione dei rischi in una sola autorità specializzata designata, con poteri di raccolta o richiesta di informazioni a fini di valutazione (si veda quanto precede riguardo alla trasparenza).[27] Le valutazioni di sicurezza dovrebbero essere schermate dall'influenza politica indiretta da parte di poteri stranieri.

2. Garantire un'efficacia legale vincolante all'atto conclusivo della valutazione del rischio, ad esempio attribuendo all'autorità il potere di emettere decisioni definitive,

[22] Voce 15 (b) della Raccomandazione.
[23] Si veda il sito di ANSSI (*l'Agence nationale de la sécurité des systèmes d'information*) https://www.ssi.gouv.fr/actualite/publication-de-larrete-du-11-aout-2016-modifiant-celui-du-4-juillet-2012-fixant-la-liste-dappareils-et-de-dispositifs-techniques-prevue-par-larticle-226-3-du-code-penal/
[24] Nuova proposta di legge francese nel *code des postes et des communications électroniques* in base alla quale gli operatori sono responsabili della richiesta di un'autorizzazione, http://www.assemblee-nationale.fr/15/propositions/pion1722.asp.
[25] Articolo 226-3 del Codice Penale (Fr: *Code Pénal*).
[26] Si veda D.Lgs. 65/2018: Link: https://www.gazzettaufficiale.it/eli/id/2018/06/09/18G00092/sg

attraverso autorizzazioni, approvazioni o licenze. Un'autorizzazione potrebbe essere soggetta a condizioni di monitoraggio e rendiconto che incentivino la *compliance*.

3. Le decisioni dell'autorità dovrebbero essere soggette ad impugnazione come in altri analoghi settori normativi, laddove richiesto dalle leggi nazionali del paese in questione.

4. Dovrebbero essere previste sanzioni proporzionate in caso di violazione, ad esempio sanzioni penali o amministrative, così come la nullità dei relativi accordi. [28]

4. Riepilogo

"Altri" Fattori	Esempio
Mancanza di trasparenza da parte del Fornitore	Il Fornitore non rivela informazioni sulla sua proprietà o sui suoi finanziamenti.
Influenza da parte di uno Stato estero: proprietà, controllo, finanziamenti, influenza politica sul Fornitore	Società possedute da uno Stato, fondi statali, rappresentanza dei partiti o concessione di influenza mediante apposite previsioni statutarie.
Norme di conflitto e efficacia extraterritoriale sul Fornitore	La "Chinese National Intelligence Law" obbliga un fornitore o un cittadino dell'UE a cooperare alla raccolta di informazioni, violando il diritto alla riservatezza delle comunicazioni e le regole del GDPR.
L'accettazione, da parte di un regime straniero, dello Stato di diritto e della separazione dei poteri	Indipendenza dei giudici e impatto del sistema giudiziario sui mezzi a disposizione del Fornitore per impugnare od opporsi alle richieste.
Misure/metodi di gestione del rischio	**Esempio**

[27] Da confrontare: https://www.dni.gov/files/NCSC/documents/products/SCRM_Framework_for_Assessing_Risk_White_Paper.pdf.

[28] Bozza di legge n. 1722 per la tutela della sicurezza nazionale e degli interessi di difesa della Francia in relazione al funzionamento delle reti mobili, presentata all'Assemblea Nazionale Francese il 20 febbraio 2019.

Base giuridica per le iniziative degli Stati Membri	L'autorità dovrebbe avere il potere di imporre agli operatori determinate condizioni nella selezione dei Fornitori.
Procedure Nazionali: autorità indipendente centralizzata, decisioni vincolanti, diritto di impugnazione, efficacia dell'applicazione attraverso sanzioni penali o amministrative	L'autorità dovrebbe essere in grado di effettuare valutazioni dei rischi in relazione ai prodotti e servizi 5G, e tali valutazioni dovrebbero divenire efficaci e operative attraverso decisioni definitive (ad esempio un'autorizzazione). La violazione di un'autorizzazione dovrebbe comportare sanzioni amministrative o penali.