Shipping Italy
Il quotidiano online del trasporto marittimo

La sicurezza del cyberspazio e la supply chain

Nicola Capuzzo · Monday, March 7th, 2022

*Contributo a cura di avv. Rosa Abbate **

** studio PG LEGAL*
VIA S. ANDREA, 3
20121 MILANO

La c.d. supply chain è un settore strategico dell'economia perché consente la movimentazione delle merci e lo svolgimento degli scambi e delle transazioni commerciali. È la catena logistica che promuove e realizza, attraverso la sua combinazione diversificata di mezzi di trasporto e tratte, la globalizzazione dell'economia reale. Quest'ultima, invero, è basata su un pilastro di fondamentale importanza dato dallo scambio e il commercio delle materie prime (c.d. commodities) indispensabili per l'economia e la vita quotidiana. Come è noto, la catena logistica è fondata sulla contestuale interazione di vari operatori (prestatori di servizi di trasporto, fornitori, produttori industrie, infrastrutture etc.etc.) e che agiscono a livello quasi prevalentemente internazionale (cioè di scambi transfrontalieri), la catena logistica che forma la supply chain è esposta, tra le altre cose, a incognite e variabili di diversa natura, non fosse altro, ad. es. alla oscillante dinamica dei mercati e dei prezzi delle materie prime oltre che dei repentini mutamenti degli assetti geopolitici.

Negli ultimi tempi, l'inaspettato fenomeno della pandemia da Covid-19 e le conseguenze sul piano della salute pubblica e dei provvedimenti adottati a livello sia nazionale che internazionale, sono state di grande impatto, così come sicuramente è e sarà il recente conflitto Russia-Ucraina. In generale dunque, e indipendentemente dagli accadimenti improvvisi quanto imprevedibili che in questi giorni sconvolgono l'intera comunità, il tema della sicurezza degli spostamenti delle merci (e delle persone) e il buon esito della spedizione senza danni e/o perdite, è imprescindibile e consolidato e si è evoluto, come è noto, da almeno un secolo nel campo della navigazione marittima (e anche aerea), prova ne è, tra l'altro, l'esistenza di specifiche regolamentazioni nazionali e internazionali (oggi anche comunitarie) che contemplano la sicurezza nella sua più ampia accezione di safety and security, della salvaguardia della vita umana in mare (tra tutte, la Convenzione SOLAS) e del rispetto dell'ambiente, del soccorso etc. etc..

La sicurezza del mezzo di trasporto e della spedizione ha, tuttavia, assunto nuovi connotati per l'avvento della tecnologia e del suo impiego capillare proprio nella navigazione marittima e aerea

e, per l'effetto, dell'intera logistica (da tempo si parla, infatti, di "logistica 4.0), e ciò ha comportato nuovi bisogni (sia in termini di prevenzione che di protezione) necessariamente estesi a settori prima mai esistiti come ad es. i "dati "e "internet" e tutto ciò che ne è derivato anche in tema di regolamentazione (ad es. in tema di tutela della privacy e la normativa GDPR). Il sistema informatico è diventato per l'economia uno strumento di lavoro e di comunicazione indispensabile e l'avvento della tecnologia in tutte le sue forme e modalità ad oggi conosciute ha comportato un mutamento radicale nei settori strategici dell'industria, delle comunicazioni, nei trasporti, nella sanità, nella finanza e perfino nella Pubblica Amministrazione.

E' significativo lo sviluppo tecnologico dei mezzi trasporto come la nave in grado di trasportare ingenti volumi di merci (ma anche di persone, come accade nel settore delle crociere) e che allo stato attuale è dotata – oramai nella quasi totalità dei casi – di apparati tecnologicamente avanzati soprattutto di tipo informatico posti al centro delle funzionalità più importanti del mezzo cui si aggiunge tutto l'apparato della connessione alle reti delle comunicazioni e geolocalizzazioni (sistema AIS, ECDIS per citare alcuni esempi). E proprio in questo senso l'esigenza di sicurezza oggi preminente è quella delle tecnologie e dell'informatica, cioè della protezione e della tutela del loro uso come strumento di lavoro in senso stretto e di comunicazione ma solo per le finalità cui sono destinate e non per altri scopi che esulano da questi ambiti per sconfinare in altri, il più delle volte di natura illecita, se non criminale o addirittura ostile.

Fra i più delicati aspetti della sicurezza oggi è proprio quello dell'uso malevolo dello strumento tecnologico e dell'informatica per il perseguimento di fini illeciti, criminali, terroristici, di atti ostili in generale, e ciò non solo a livello politico ma anche economico, come lo spionaggio industriale, la concorrenza sleale, il furto e/o la manomissione dei dati, nonché sociale come ad es. la manipolazione delle informazioni (c.d. fake news) e degli strumenti di comunicazione. In questo senso la c.d. cybersicurezza è l'esigenza contemporanea di necessaria e opportuna tutela dell'impiego della tecnologia, la best practice da implementare ed aggiungere come sistema all'organizzazione sia aziendale che istituzionale. Lo spazio "cibernetico"(cyberspace) è un ecosistema che non ha confini ed è caratterizzato da molteplici funzioni quanto al suo impiego a alle presenze di soggetti che operano in questo ambiente: si pensi alle connessioni internet oramai imprescindibili per gli scambi e/o le operazioni commerciali e finanziarie – sempre più spesso traslate dal reale al virtuale -, il lavoro da remoto, la didattica a distanza, la telemedicina, le molteplici e variegate attività e funzioni della pubblica amministrazione.

L'evidenza dell'uso sempre più massiccio e capillare della tecnologia e, più in generale, della veloce transizione del sistema tradizionale verso quello tecnologico ed informatizzato, si può constatare non solo sul piano economico e commerciale ma anche e già da un po' di tempo proprio in Italia a livello normativo e di pubblica amministrazione come dimostra, per citare qualche esempio, l'entrata in vigore delle Linee Guida dell'AGID (Regolamento per l'adozione di linee guida per l'attuazione del Codice dell'Amministrazione Digitale di cui al decr. Legsl. 7.3.2005 n. 82) e la (prima forma di) regolamentazione sugli "smart contracts" oggetto dell'art. 8-ter decreto semplificazioni del 2019. Il cyberspazio può, dunque, essere importante per lo sviluppo ed il progresso ma allo stesso tempo essere anche fonte di gravi pericoli per la sicurezza in generale e di minaccia per la stabilità ed il funzionamento dell'innovazione tecnologica e la transizione digitale. Questo fenomeno negativo è stato da tempo messo in evidenza dagli esperti del settore e recepito dagli organi di governo come emerge, tra l'altro, dalla Relazione Sulla Politica dell'Informazione per la Sicurezza del 2021 presentata in Parlamento (www.sicurezzanazionale.gov.it) nonché dalla recente istituzione nel nostro Paese dell'Agenzia per la Cybersicurezza Nazionale – ACN di cui alla L. 4.8.2021 N. 109 che opera come autorità nazionale a tutela degli interessi della

cybersicurezza e ove, tra le altre cose, è costituito in via permanente il Nucleo per la cybersicurezza che supporta il Capo di Governo per gli aspetti relativi alla prevenzione e preparazione a eventuali situazioni di crisi e per l'attivazione di procedure per l'allertamento. Le azioni criminali da parte di hacker informatici si sono già da tempo intensificate per effetto della pandemia, ove si è potuta registrare una sensibile crescita di azioni cyber di matrice criminale basate su attacchi di tipo ramsonware (tra questi, esponenziale l'aumento degli attacchi RaaS, Ramsonwas as a service) accompagnati sovente da richieste estorsive di denaro. In tal senso, gli esperti della cybersicurezza hanno posto in risalto in vari studi che nel 2021 si è registrato un aumento fino al doppio rispetto al 2020 del numero di attacchi ramsonware, del numero dei gruppi criminali presenti nel dark web e dei costi di recupero da ramsonware.

Nella predetta Relazione si evidenzia, tra l'altro, che le attività criminali hanno riguardato sia il settore pubblico, interessando anche le amministrazioni centrali dello stato e infrastrutture IT di enti locali e strutture sanitarie, sia i soggetti privati con prevalenza per il settore energetico, delle telecomunicazioni e dei trasporti, il tutto con un trend in crescita rispetto a 2020. Addirittura, secondo uno studio dell'Osservatorio Cybersuceurity Exprivia, il 2021 è stato un annus horrbilis per l'aumento degli attacchi informatici ai danni di aziende italiane, di incidenti, violazioni della privacy e sottrazione di dati perpetrati anche con tecniche "miste". A questo va aggiunto inevitabilmente il conflitto Russia-Ucraina esploso in questi giorni che ha acuito in modo esponenziale i problemi della cybersicurezza ponendone ulteriori e più gravi stante il concreto rischio di attacchi informatici come strumento offensivo da parte di hacker (attivisti o altri gruppi) volti a colpire infrastrutture IT nazionali e internazionali e i mezzi di informazione a scopi belligeranti. Secondo gli esperti lo spazio cyber costituisce un nuovo scenario di scontro e sembra potersi considerare come "quinto dominio di guerra dopo aria, terra, mare e spazio".

A tale proposito, l'interessante pubblicazione del Bollettino di sicurezza dello CSIRT Italia (BL01/220228/CSIRT-ITA del 28.2.2022) rivolto a tutti gli operatori di infrastrutture digitali nazionali in cui si raccomanda di innalzare "la postura difensiva" e di adottare massima difesa cibernetica a causa dell'incremento di nuovi attacchi informatici criminali (come ad es. attraverso HermeticWiper) volti alla distruzione dei dati e a minare la continuità dei servizi essenziali. In tale generale contesto è coinvolta l'intera catena logistica della supply chain il cui funzionamento non può prescindere da una adeguata preparazione e predisposizione di sistemi di sicurezza informatica, monitoraggio interno ed esterno ai processi aziendali e controllo dei possibili incidenti nonché di ripristino delle funzionalità e recupero dei dati, e tale esigenza renderebbe opportuna una sua implementazione a livello di risk management.

Rosa Abbate

This entry was posted on Monday, March 7th, 2022 at 8:30 am and is filed under Economia, Market report
You can follow any responses to this entry through the Comments (RSS) feed. Both comments and pings are currently closed.