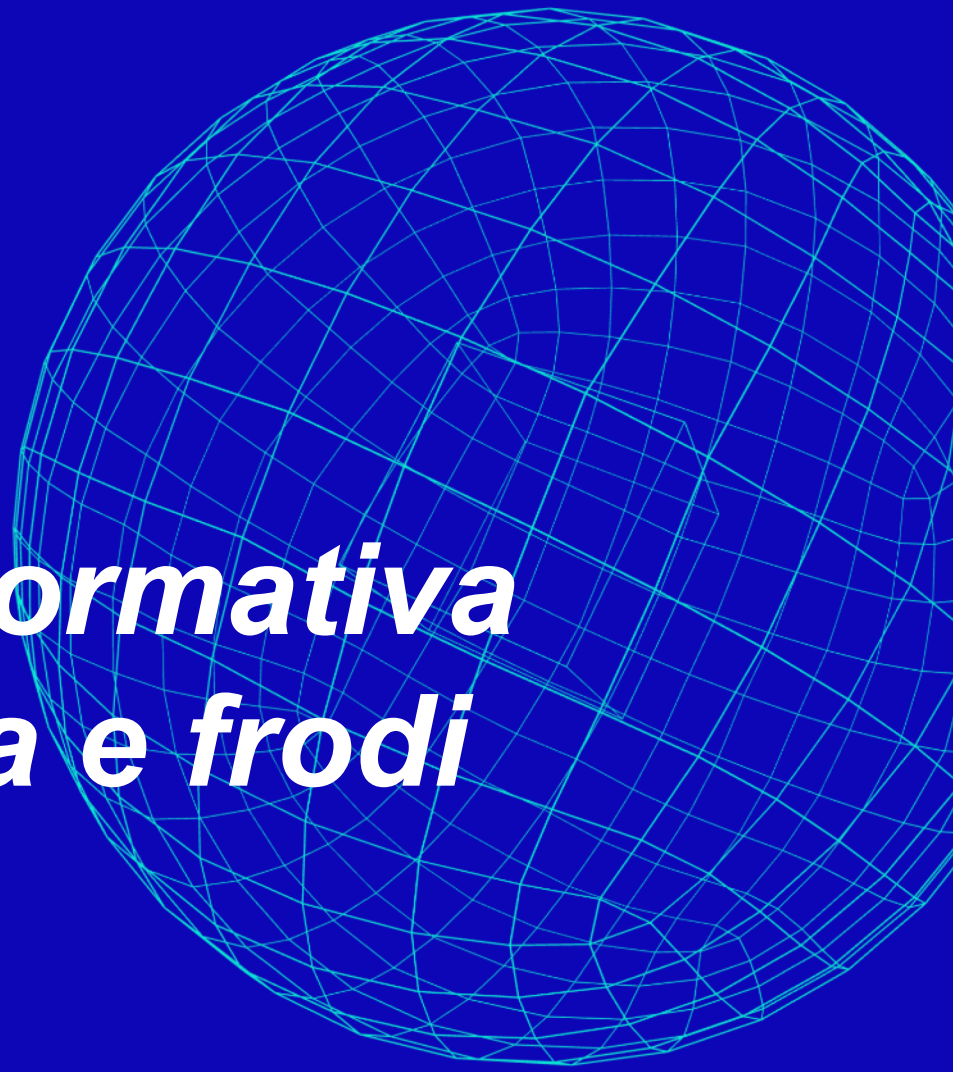
CERTFin

14 maggio 2024

Lo stato dell'arte della normativa in ambito cybersicurezza e frodi informatiche



Maria Ferrucci

Cyber security and fraud Analyst

La cybersicurezza e le frodi informatiche…nella letteratura

CERTFin

La Direttiva NIS (2016/1148) definisce la sicurezza della rete e dei sistemi informativi (**cybersicurezza**) come «*la capacità di una rete e dei sistemi informativi di resistere, a un determinato livello di riservatezza, a ogni azione che comprometta la disponibilità, l'autenticità, l'integrità o la riservatezza dei dati conservati o trasmessi o trattati e dei relativi servizi offerti o accessibili tramite tale rete o sistemi informativi.*»

Gli Orientamenti EBA in materia di segnalazione per i dati sulle frodi (EBA/GL/2018/05) classificano le **operazioni di pagamento fraudolente** come:

- **Operazioni non autorizzate**:
  - emissione di un ordine di pagamento da parte del frodatore → *«il frodatore emette un falso ordine di pagamento dopo aver ottenuto i dati di pagamento sensibili del pagatore/beneficiario con mezzi fraudolenti»*
  - modifica di un ordine di pagamento da parte del frodatore → *«il frodatore intercetta e modifica un ordine di pagamento legittimo durante la trasmissione elettronica tra il dispositivo del pagatore e il prestatore di servizi di pagamento (per esempio tramite malware o attacchi che consentono agli aggressori di intercettare la comunicazione tra due host legittimamente comunicanti, attacchi «man-in-the middle») oppure modifica l'istruzione di pagamento nel sistema del prestatore di servizi prima che il relativo ordine sia compensato e regolato»*
- **Operazioni autorizzate** (manipolazione del pagatore) → *«operazioni di pagamento effettuate in conseguenza di una manipolazione operata dal frodatore a danno del pagatore allo scopo di indurlo a emettere un ordine di pagamento, o impartire un'istruzione di pagamento al prestatore di servizi di pagamento, in buona fede, su un conto che egli ritiene appartenere a un beneficiario legittimo»*

Stato dell'arte della normativa: il contesto internazionale

CERTFin

Principale framework normativo in ambito cybersecurity e frodi informatiche e recenti iniziative in perimetro

- **PSD2** (2015)
- **GDPR** (2016)
- **Direttiva NIS** (2016)
- **RTS su SCA e CSC** (2017)
- **GL EBA sulla segnalazione dei dati sulle frodi** ai sensi dell'art. 96(6) della PSD2 (20
- **EUCSA** (2019)
- **GL EBA sulla gestione dei rischi ICT e di sicurezza** (2019)
- **GL EBA in materia di segnalazione dei gravi incidenti** ai sensi della PSD2 (2021)
- **Direttiva CER** (2022)
- **Direttiva NIS2** (2022)
- **DORA** (2022)
- **CRA** (proposta, 2022)
- **PSR e PSD3** (proposte, 2023)
- **Regolamento sui bonifici istantanei** (2024)
- **Regolamento eIDAS 2.0** (2024)

Ulteriori recenti riferimenti:

- BCBS DP ***Digital fraud and banking: supervisory and financial stability implications*** (2023)
- EBA ***Opinion on new types of payment fraud and possible mitigants*** (2024)

Ulteriori recenti iniziative:

- ***ERPB WG on fraud related to retail payments***
- ***European Forum on the***

Stato dell'arte della normativa: il contesto nazionale

CERTFin

Principale framework normativo in ambito cybersecurity e frodi informatiche

- **Quadro Strategico Nazionale** per la sicurezza dello spazio cibernetico e Piano nazionale per la protezione cibernetica e la sicurezza informatica (DPCM 24 gennaio 2013)
- Attuazione della **Direttiva NIS** (D.lgs. 18 maggio 2018, n.65)
- **Perimetro di sicurezza cibernetica** (DL 21 settembre 2019 n.105, convertito L.18 novembre 2019, n.133)
- **Regolamento in materia** di perimetro di sicurezza nazionale (DPCM 30 luglio 2020, n.131)
- Regolamento in materia di **notifiche degli incidenti** aventi impatto su reti, sistemi informativi e servizi informatici (DPCM 14 aprile 2021, n.81)
- **Individuazione beni, sistemi e servizi ICT** del Perimetro e istituzione del **CVCN** (DPCM 15 giugno 2021)
- **Disposizioni urgenti** in materia di cybersicurezza, definizione dell'**architettura nazionale** di cybersicurezza e **istituzione dell'ACN** (DL 14 giugno 2021, n. 82, convertito in L. 4 agosto 2021, n.109)
- **Strategia Nazionale di cybersicurezza 22-26** e relativo Piano di implementazione (DPCM 17 maggio 2022)
- Adeguamento al Regolamento EUCSA (D.lgs. 3 agosto 2022, n.123)
- **Tassonomia** degli incidenti che debbono essere oggetto di notifica (Determina ACN 3 gennaio 2023)
- Disposizioni in materia di **rafforzamento della cybersicurezza nazionale** e di reati informatici (DDL

- **Circolare 285/2013 Banca d'Italia**

CERTFin

Grazie!

EBA Opinion on new types of payment frauds and possible mitigants

CERTFin

NEW TYPES OF PAYMENT FRAUD

- Manipulation of the payer
- Mixed social engineering and techical scam
- Enrollment process compromise

POSSIBILE MITIGANTS

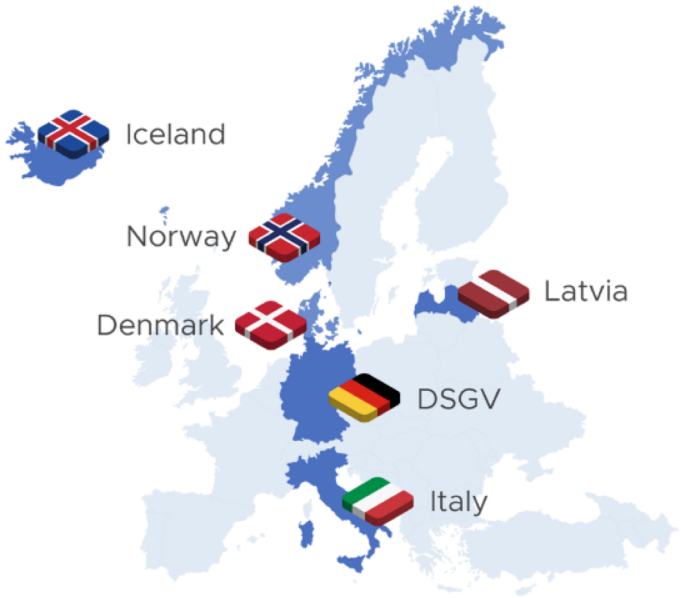
- Reinforced security requirements for PSPs
- A fraud risk management framework to be put in place by PSPs
- Amended liability rules
- Strenghten and harmonize the supervision of fraud management
- Security requirements for a single EU-wide platform for information sharing

Il progetto europeo NOBID

CERTFin

Il progetto **NOBID** (Nordic-Baltic eID) è uno dei 4 progetti pilota sull'identità digitale finanziati dal programma *DIGITAL Europe* dell'UE e che coinvolgono circa 360 soggetti, tra cui imprese private e autorità pubbliche di 26 Stati membri. **ABI Lab** è uno dei partner del consorzio.

La Commissione Europea ha fornito un prototipo di **portafoglio di identità digitale (EUDI)**, conforme ai requisiti del regolamento eIDAS, che sarà testato attraverso i progetti pilota.



In particolare NOBID:

- è stato avviato a maggio 2023 e durerà 2 anni
- ha l'obiettivo di impiegare il portafoglio di identità digitale dell'UE per **autorizzare pagamenti di prodotti e servizi**

The NOBID Consortium is Co Funded by the European Union, as part of the Digital Europe Work Programme 2021-2022, and is one of four Large Scale Pilots funded after the call for Accelerating best use of technologies (DIGITAL-2022-DEPLOY-02)

CERTFin

Grazie!