07
OTTOBRE
2021

NEWSADP

NEWSLETTER SU AMMINISTRAZIONE DIGITALE E PRIVACY
A CURA DEL PROF. AVV. MARCO MANCARELLA DI CONCERTO CON LA RITT

www.liquidlaw.it
@liquidlawsrl
liquidlaw

liquid LAW spin-off UNIVERSITÀ DEL SALENTO
DH CENTRO INTERDIPARTIMENTALE DI RICERCA
MODiCT Centro di ricerca del Dipartimento di Storia, Società e Studi sull'Uomo

SMART WORKING PA: LINEE GUIDA BRUNETTA

Lo schema delineato nella bozza delle nuove regole indica l'obbligo, da parte del datore di lavoro, di fornire al lavoratore abbonamento Internet oltre a un'idonea dotazione tecnologica. Sembra, inoltre, sia stato eliminato il tetto massimo di lavoratori che possono accedere alla prestazione lavorativa "agile". Garantiti, infine, nella bozza il diritto alla disconnessione, la privacy e le regole per lavorare dall'estero. I sindacati sono divisi. Le Linee Guida passano ora al vaglio della Conferenza unificata.

ARGOMENTO E TEMI TRATTATI
da Federica Meta nell'articolo "Smart working nella PA, ecco le linee guida di Brunetta":
https://www.corrierecomunicazioni.it/lavoro-carriere/smart-working/smart-working-nella-pa-ecco-le-linee-guida-di-brunetta/

SICUREZZA: MONITORAGGIO SISTEMI PA

Nuova rilevazione, a cura di AgID, sull'utilizzo del protocollo HTTPS e sull'aggiornamento dei CMS nei sistemi della PA, come previsto dal Piano Triennale per l'informatica nella Pubblica Amministrazione. Se, da un lato, la percentuale di siti che utilizza una corretta configurazione HTTPS è più che raddoppiata, dall'altro, quella dei CMS aggiornati evidenzia un peggioramento.
I siti monitorati sono quella della Pubblica Amministrazione disponibile nell'Indice PA (IPA). Nonostante la valutazione della sicurezza dei sistemi della PA non possa basarsi solo sulla misurazione del numero di enti che hanno il CMS aggiornato e la configurazione del protocollo HTTPS sicura, questi due aspetti sono, a ogni modo, significativi ed indicativi della diffusione della cultura della cibersicurezza nazionale, in particolare nelle amministrazioni.

PUBBLICATO SU:
https://www.agid.gov.it/it/agenzia/stampa-e-comunicazione/notizie/2021/10/22/sicurezza-i-risultati-del-secondo-monitoraggio-sui-sistemi-pa

CYBERSICUREZZA, STRATEGIA UE: DOVE SI INCEPPA IL MECCANISMO?

Il 7 ottobre scorso, il Parlamento europeo ha approvato la relazione della Commissione Europea contenente un progetto volto a instaurare una maggior cooperazione e adottare un piano comune in tema di difesa del cyber spazio, non limitandosi ad una postura difensiva.
Tuttavia, la Comunità Europea deve fare i conti con: vuoti normativi; limitati investimenti nel settore informatico (dovuti, in parte, all'insufficienza dei fondi ma, principalmente, alla carenza di esperti del settore); sviluppo disomogeneo delle tecnologie e delle politiche ad esse correlate nei 27 Stati membri. Fattori che concorrono a rellentare l'UE nella realizzazione di un quadro giuridico europeo unico e nel raggiungimento di un adeguato grado di efficienza nella cooperazione tra gli Stati membri.

ARGOMENTO E TEMI TRATTATI
da Gianluca Fabrizi e Lorenzo Fortunati nell'articolo "Cybersicurezza: la strategia Ue per una difesa comune, tra lacune normative e pochi fondi":
https://www.agendadigitale.eu/sicurezza/cybersicurezza-la-strategia-ue-per-una-difesa-comune/

COPYRIGHT, SCHEMA DI DECRETO: OK DEL PARLAMENTO

Arrivati i pareri positivi delle Commissioni di Senato e Camera allo schema di decreto legislativo sul copyright. Si attende a breve l'ok da parte del Governo presieduto da Mario Draghi.
Durante un'intervista di qualche giorno fa, Francesco Posteraro, ex Commissario Agcom, dichiarava che "(...) la rete deve essere adeguatamente regolamentata, al pari di ogni ambito nel quale si svolge l'attività umana. Quello che non è lecito nello spazio fisico non può diventare lecito nello spazio virtuale: oggi sembra un'ovvietà, ma in passato abbiamo faticato non poco per farlo intendere a molti, perfino nel mondo politico."

ARGOMENTO E TEMI TRATTATI
da Fabio Fabbri nell'articolo "Copyright: ok dal Parlamento allo schema di decreto, rafforzato il ruolo dell'Agcom":
https://www.key4biz.it/copyright-ok-dal-parlamento-allo-schema-di-decreto-agcom-piu-forte/378714/

IDENTITÀ DIGITALE UNICA: UNA PARTITA ANCORA APERTA

Dall'1 ottobre, ai servizi online della PA si accede obbligatoriamente con SPID, CIE, CNS. La normativa di riferimento è contenuta nel DL 76/2020.
L'obbligo, però, riguarda, ad oggi, solo i cittadini. Reintrodotta per professionisti e imprese la norma [comma 3-bis dell'articolo 64 del codice dell'amministrazione digitale (D. Lgs. 82 del 2005)], che affida a un Dpcm oppure a un decreto del ministro dell'innovazione il compito di fissare la data dello switch off.
Sebbene si tratti del primo grande passo verso la completa digitalizzazione delle comunicazioni tra cittadino e Amministrazione, molti sono ancora i tasselli da sistemare.

ARGOMENTO E TEMI TRATTATI
da Patrizia Saggini nell'articolo "Identità digitale unica, dopo il primo ottobre cosa resta da fare":
https://www.agendadigitale.eu/cittadinanza-digitale/identita-digitale/spid-e-identita-digitale-cosa-e-cambiato-dal-primo-ottobre-e-cosa-resta-da-sistemare/

DELEGHE SPID: COME GESTIRLE?

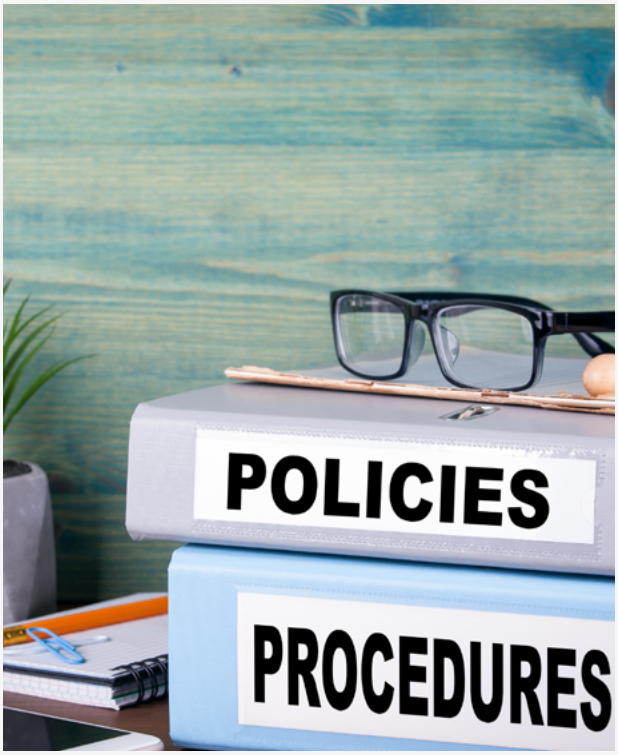
Cosa fare e come fare nel caso di cittadini impossibilitati all'utilizzo autonomo dei servizi on-line della PA? Si pensi ad alcuni servizi come, ad esempio, quelli di Inps, relativamente ai quali numerosi pensionati delegano figli e nipoti. Situazione che ha portato gli operatori a concentrarsi sull'individuazione delle modalità di gestione degli accessi da parte dei cittadini, avvalendosi di un intermediario appositamente delegato a tal fine.

ARGOMENTO E TEMI TRATTATI
da Alessandro Mastromatteo nell'articolo "Deleghe Spid, ecco come gestirle su Inps e non solo": *https://www.agendadigitale.eu/cittadinanza-digitale/identita-digitale/spid-per-i-cittadini-ecco-come-gestire-le-deleghe/*

DECRETO CAPIENZE: PRIVACY IN PERICOLO?

Approvato dal Consiglio dei ministri giovedì 7 ottobre 2021, il Decreto Capienze prevede un allentamento delle restrizioni imposte a luoghi quali discoteche, cinema, teatri. Esso dispone altresì l'impiego di Green pass e mascherine oltre a stabilire le percentuali di affluenza consentite nei luoghi di cui sopra.
Una parte del decreto, tuttavia, sta suscitando grande preoccupazione presso gli esperti privacy. Si tratta dell'articolo 9, nel quale si indica che: **1.** il trattamento dei dati da parte delle PA è sempre consentito per finalità pubbliche; **2.** se la finalità del trattamento non è prevista dalla legge, la PA con un atto amministrativo potrà indicarla e svolgere il trattamento che ritiene necessario; **3.** il Garante privacy non potrà più svolgere controlli preventivi nel caso di trattamenti di dati ad alto rischio (abrogando, così, l'articolo 2 quinquiesdecies del Codice Privacy).

PUBBLICATO SU:
https://www.entilocali-online.it/decreto-aperture-e-privacy-chiarezza-sulle-p-a-ma-limitazioni-al-garante-sul-pnrr/



ARGOMENTO E TEMI TRATTATI
da Sabatina De Fusco e Giorgio Iorio nell'articolo "Se la ricerca scientifica usa dati rubati: le implicazioni etiche e morali": *https://www.agendadigitale.eu/sicurezza/dati-rubati-usati-nella-ricerca-scientifica-le-implicazioni-etiche-e-morali/*

DATI: E SE A RUBARLI È LA RICERCA SCIENTIFICA?

Da un'indagine condotta da Ibm Security su 21 aziende italiane è emerso che nel 2020, il costo complessivo delle violazioni di dati è salito a 3,03 milioni di euro e il costo per ogni informazione rubata a 135 euro, valore quasi raddoppiato nell'ultimo decennio. Nel solo 2020, in Italia sono stati rubati in totale 24mila record. I settori maggiormente colpiti dagli attacchi informatici sono stati i servizi finanziari, il settore energetico e, infine, quello farmaceutico. Poco confortante anche il fatto che sono necessari ancora 250 giorni per identificare e contenere una minaccia informatica. Cosa succede, però, quando i dati rubati vengono resi pubblici e utilizzati per la ricerca scientifica? Quali le implicazioni etiche e morali?

GREEN PASS E GRANDI AZIENDE: COME FUNZIONA SUL SITO DELL'INPS?

'Greenpass50+' è il servizio per la verifica del Green pass, pubblicato sul sito dell'Inps, dedicato ad aziende private con più di 50 dipendenti e ad enti pubblici (scuole escluse) non aderenti a NoiPA, a prescindere dal numero di dipendenti. Tre le fasi previste dal servizio: **1.** di accreditamento; **2.** elaborativa; **3.** di verifica.
I verificatori accedono con SPID, il server viene interrogato di notte con modalità asincrona e i dati vengono cancellati dopo 24 ore.

ARGOMENTO E TEMI TRATTATI
da Luigi Garofalo nell'articolo "Green pass, come funziona sul sito dell'Inps la verifica per grandi aziende": *https://www.key4biz.it/green-pass-come-funziona-sul-sito-dellinps-verifica-per-grandi-aziende/378880/*

OSPEDALI: VITTIME PERFETTE DEI CYBERCRIMINALI

Furto di dati e attacchi informatici in ambito sanitario hanno registrato una forte impennata, soprattutto dall'inizio della pandemia, poiché i dati sanitari che trattano rappresentano una merce preziosissima. Una vulnerabilità, quella delle strutture ospedaliere, spesso sottovalutata cui seguono deboli azioni di difesa cibernetica. Situazioni che possono passare inosservate sino a quando non si verificano attacchi ransomware come quello che ha colpito lo Springhill Medical Center, in Alabama, il cui drammatico epilogo dovrebbe quantomeno insegnarci quanto gli ospedali restino un bersaglio che vale la pena proteggere. Le ripercussioni, infatti, non sono da calcolare solo in termini di danni economici e reputazionali, ma anche sanitari e legati alla salute.

ARGOMENTO E TEMI TRATTATI
da Virginia Sacco nell'articolo "Ospedali sotto attacco cyber: perché sono vittime perfette":
https://www.agendadigitale.eu/sicurezza/ospedali-sotto-attacco-hacker-ragioni-e-vulnerabilita-che-li-rendono-target-perfetti/