DETERMINAZIONE N. 364/2020

Oggetto: Approvazione della Trattazione n. 120/2019 e Comunicazione n. 120/2019 riguardante la Segnalazione all'Ufficio del Difensore civico per il digitale n. 120/2019 prot. n. 13887 del 18/10/2019.

IL DIRETTORE GENERALE

VISTI gli articoli 19 (Istituzione dell'Agenzia per l'Italia Digitale), 21 (Organi e statuto), 22 (Soppressione di DigitPA e dell'Agenzia per la diffusione delle tecnologie per l'innovazione; successione dei rapporti e individuazione delle effettive risorse umane e strumentali) del decreto legge n. 83 del 22 giugno 2012, recante "Misure urgenti per la crescita del Paese", convertito, con modificazioni, nella legge n. 134 del 7 agosto 2012 e s.m.i. e l'articolo 14-bis (Agenzia per l'Italia digitale) nonché l'articolo 17, (Responsabile per la transizione digitale e difensore civico digitale) del decreto legislativo n. 82 del 7 marzo 2005 (Codice dell'amministrazione digitale) e s.m.i. e, in particolare, il comma 1-quater del suddetto articolo 17 ai sensi del quale è istituito presso l'AgID l'ufficio del difensore civico per il digitale;

VISTO il decreto del Presidente del Consiglio dei Ministri dell'8 gennaio 2014 (pubblicato sulla GURI n. 37 del 14 febbraio 2014), che ha approvato lo Statuto dell'Agenzia per l'Italia Digitale (AgID);

VISTO il decreto del Presidente del Consiglio dei Ministri 9 gennaio 2015, pubblicato nella Gazzetta Ufficiale n. 82 del 9 aprile 2015, concernente la "Determinazione delle dotazioni delle risorse umane, finanziarie e strumentali dell'Agenzia per l'Italia digitale", adottato ai sensi dell'articolo 22, comma 6, del decreto-legge n. 83 del 2012;

VISTO il decreto del Presidente del Consiglio dei Ministri in data 27 marzo 2017, recante "Approvazione del regolamento di organizzazione per l'Agenzia per l'Italia Digitale";

VISTO il decreto del Presidente del Consiglio dei Ministri del 16 gennaio 2020, registrato alla Corte dei Conti in data 17 febbraio 2020 al n. 232, con cui l'ing. Francesco Paorici è stato nominato, per la durata di un triennio, Direttore Generale dell'Agenzia per l'Italia Digitale, con decorrenza dal 20 gennaio 2020;

VISTA la determinazione n. 15/2018 del 26/1/2018 con la quale si stabilisce che, in attuazione dell'articolo 17 comma 1-quater del decreto legislativo n. 82/2005 e s.m.i., è istituito presso l'AgID l'Ufficio del difensore civico per il digitale, al quale è preposto il dott. Massimo Macchia, che si avvarrà del personale in servizio presso l'ufficio Affari Giuridici e Contratti e che le aree tecniche presteranno

supporto al Difensore civico digitale al fine di fornire al medesimo elementi utili in ordine alle segnalazioni ricadenti nelle aree di propria competenza;

VISTO l'articolo 66 comma 2 del d.lgs. 217/17 ove, tra l'altro, si prevede che, "*al fine di garantire una tempestiva ed efficace attuazione del decreto legislativo n. 82 del 2005, e, in particolare, di svolgere le attività previste dall'articolo 17, comma 1-quater e dall'articolo 71 del predetto decreto legislativo e le altre misure aggiuntive disposte dal presente decreto, l'AgID può avvalersi, in aggiunta alla dotazione organica vigente, di un contingente di 40 unità di personale di altre amministrazioni statali, in posizione di comando o fuori ruolo, ai sensi dell'articolo 17, comma 14, della legge 15maggio 1997, n. 127*";

VISTA la determinazione n. 37 del 12/02/2018 con la quale è stato approvato il Regolamento concernente le procedure interne all'Agenzia per l'Italia digitale aventi rilevanza esterna, finalizzate allo svolgimento, nella fase di prima applicazione, dei compiti previsti dall'articolo 17, comma 1-quater del Codice dell'Amministrazione digitale, relativi al Difensore civico per il digitale;

VISTA la segnalazione al Difensore civico per il digitale n. 120/2019 del 18/10/2019 acquisita al prot. n. 13887 del 18/10/2019, con la quale un Ordine professionale rappresentava criticità operative di interazione con i siti istituzionali di PP.AA. non dotati della cifratura di canale tramite i protocolli HTTPS/TLS, a seguito dell'adeguamento della struttura informatica e del sito alle misure minime di sicurezza.;

ESAMINATA la Trattazione n. 120/2019, predisposta dall'Ufficio del Difensore civico per il digitale, relativa all'esame istruttorio della tematica di cui al sopra riportato articolo, per la quale si propone l'archiviazione in quanto risulta che la comunicazione in argomento non si ritiene risponda ai criteri indicati dall'art. 17 comma 1-quater del CAD, bensì possa considerarsi come richiesta di informazioni;

ESAMINATA la comunicazione di Archiviazione n.120/2019, conseguente all'approvazione da parte del Difensore per il digitale della proposta di archiviazione contenuta nella richiamata Trattazione n.120/2019, trasmessa al Direttore Generale per quanto di competenza e, qualora nulla osti, con archiviazione della Segnalazione e comunicazione al Segnalante;

DETERMINA

di approvare dette Trattazione n. 120/2019 ed Archiviazione di seguito allegate, che formano parte integrante della presente determinazione.

FRANCESCO PAORICI

Firmato digitalmente da FRANCESCO PAORICI
Data: 2020.08.24 15:58:28 +02'00'

Segnalazione n. 120/2019 - Trattazione

Oggetto: Amministrazione segnalata: PP.AA. - Qualificazione tematica: Uso delle tecnologie - Protocollo n. 13887 del 18/10/2019.

La Segnalante espone quanto segue: "*Buonasera. Sono dipendente di un Ordine professionale che ha adeguato la struttura informatica e il sito alle misure minime di sicurezza e linea guida Agid e questo ci impedisce di accedere a siti non sicuri. Dobbiamo purtroppo constatare che la maggior parte delle piattaforme della PA a cui dobbiamo accedere per adempiere a obblighi normativi risultano "non sicuri" e inaccessibili. I nostri tecnici e l'amministrazione di sistema ritengono, e condivido, che non si possa fare diversamente. Di fatto lavorare sta diventando un problema. Possiamo fare qualcosa? Grazie*".

Da quanto rappresentato si evidenziano criticità operative di interazione con i siti istituzionali di PP.AA. non dotati della cifratura di canale tramite i protocolli HTTPS/TLS, a seguito dell'adeguamento della struttura informatica e del sito alle misure minime di sicurezza.

Si deve primariamente considerare che il Difensore civico per il digitale ha il compito di raccogliere tutte le segnalazioni relative alle presunte violazioni del Codice dell'Amministrazione Digitale, o di ogni altra norma in materia di digitalizzazione ed innovazione, a garanzia dei diritti digitali dei cittadini e delle imprese. L'Ufficio del Difensore civico per il digitale è stato istituito presso AgID con l'articolo 17, comma 1-quater del citato Codice.

A seguire preme osservare che il Difensore non risolve o media eventuali controversie tra il cittadino e la Pubblica Amministrazione; non può sostituirsi alla pubblica amministrazione nell'espletamento dell'attività richiesta dal cittadino; non svolge attività di supporto riguardo il malfunzionamento di soluzioni applicative utilizzate dalle pubbliche amministrazioni per l'erogazione di servizi on line (non è un servizio di *help desk*); non sostituisce l'Ufficio per i rapporti con il pubblico presente in ciascuna amministrazione.

Tanto riportato, si precisa che la comunicazione in argomento non si ritiene risponda ai criteri indicati dall'art. 17 comma 1-quater del CAD, ossia non è relativa a presunte violazioni del CAD e di ogni altra norma in materia di digitalizzazione ed innovazione della pubblica amministrazione. Per tale motivo detta comunicazione si ritiene possa considerarsi come richiesta di informazioni e non

come segnalazione, con conseguente proposta di ritenere la stessa non ricevibile, con conseguente archiviazione.

Al fine di fornire comunque un supporto informativo si ricorda che le misure minime di sicurezza sono un importante supporto metodologico oltre che un mezzo attraverso il quale le Amministrazioni, soprattutto quelle più piccole e con minor possibilità di avvalersi di professionalità specifiche, possono verificare autonomamente la propria situazione ed avviare un percorso di monitoraggio e miglioramento. In termini pratici, l'applicazione delle misure minime serve a ridurre al minimo i rischi di:

- accessi non autorizzati ai sistemi;
- trattamento di dati non consentiti o non conformi alle normali finalità;
- modifica di dati in conseguenza di interventi non autorizzati o non conformi alle regole;
- distruzione o perdita, anche accidentale, di dati.

Pertanto, le stesse stabiliscono una base comune di misure tecniche ed organizzative irrinunciabili nell'attuale contesto del mondo ICT, nel quale è in costante aumento il rischio di minacce cibernetiche soprattutto nel mondo della PA, da sempre in possesso di dati di grande valore specifico.

Tecnicamente le misure minime sottolineano comunque quelle che dovrebbero essere le comuni regole di buon senso (nonché *best practices* internazionalmente riconosciute) nella conduzione ed organizzazione dei sistemi ICT e, di per sé, la loro implementazione non dovrebbe normalmente creare alcun tipo di problema tecnico od organizzativo. Il fatto che, nonostante sia ormai altamente sconsigliato, alcune amministrazioni utilizzino ancora siti ed accessi non dotati della cifratura di canale tramite i protocolli HTTPS/TLS è da considerarsi una cattiva pratica che sia AgID sia il CERT-PA contrastano con quelli che sono i mezzi a loro disposizione e che, a poco a poco, auspicabilmente andrà scomparendo, anche perché pesantemente osteggiato anche dai software di uso più comune.

Di conseguenza, né AgID né il Cert-PA suggeriscono di abbassare i controlli minimi di sicurezza in favore di un'ipotetica maggior facilità operativa poiché le Amministrazioni, in quanto in caso di incidente informatico dovuto all'inosservanza delle stesse, le stesse Amministrazioni potrebbero essere chiamate a risponderne direttamente.

Nel caso in cui ci si imbatta in un sito e/o servizio non conforme agli attuali *standard* di utilizzo sicuro, l'invito è quello di comunicare secondo le modalità disponibili al *link* https://www.cert-pa.it/segnalazioni/ le coordinate del servizio stesso, in modo da attuare i passi opportuni per la risoluzione/mitigazione della problematica riscontrata.

Alla luce di quanto riportato, si ritengono terminate le attività istruttorie e si propone di ritenere la trattazione conclusa, con comunicazione al Direttore Generale per quanto di competenza e, qualora nulla osti, con archiviazione della medesima dandone notizia all'utente.

16 aprile 2020 Simone Rovelli

AGID
Agenzia per l'Italia Digitale

Ufficio del difensore civico per il digitale

Oggetto: Comunicazione relativa alla Segnalazione n. 120/2019 - Amministrazione segnalata: PP.AA. - Qualificazione tematica: Uso delle tecnologie - Protocollo n. 13887 del 18/10/2019.

Gent.ma Segnalante, si riporta quanto da Lei rappresentato: "*Buonasera. Sono dipendente di un Ordine professionale che ha adeguato la struttura informatica e il sito alle misure minime di sicurezza e linea guida Agid e questo ci impedisce di accedere a siti non sicuri. Dobbiamo purtroppo constatare che la maggior parte delle piattaforme della PA a cui dobbiamo accedere per adempiere a obblighi normativi risultano "non sicuri" e inaccessibili. I nostri tecnici e l'amministrazione di sistema ritengono, e condivido, che non si possa fare diversamente. Di fatto lavorare sta diventando un problema. Possiamo fare qualcosa? Grazie*".

Si ricorda che il Difensore civico per il digitale ha il compito di raccogliere tutte le segnalazioni relative alle presunte violazioni del Codice dell'Amministrazione Digitale, o di ogni altra norma in materia di digitalizzazione ed innovazione, a garanzia dei diritti digitali dei cittadini e delle imprese. L'Ufficio del difensore civico per il digitale è stato istituito presso AgID con l'articolo 17, comma 1-quater del Codice dell'Amministrazione Digitale. I principali ambiti di tutela per il cittadino e le imprese riguardano l'uso delle tecnologie, l'identità digitale, il domicilio digitale, i pagamenti con le modalità informatiche e la comunicazione mediante le tecnologie dell'informazione.

Inoltre, si specifica che il Difensore non risolve o media eventuali controversie tra il cittadino e la pubblica amministrazione; non può sostituirsi alla pubblica amministrazione nell'espletamento dell'attività richiesta dal cittadino; non svolge attività di supporto riguardo il malfunzionamento di soluzioni applicative utilizzate dalle pubbliche amministrazioni per l'erogazione di servizi *on line* (non è un servizio di *help desk*); non sostituisce l'Ufficio per i rapporti con il pubblico presente in ciascuna amministrazione.

Venendo a quanto da Lei rappresentato, si evidenziano criticità operative di interazione con i siti istituzionali di PP.AA. non dotati della cifratura di canale tramite i protocolli HTTPS/TLS, a seguito dell'adeguamento della struttura informatica e del sito alle misure minime di sicurezza.

Ne deriva, quindi, che la Sua comunicazione non è relativa a presunte violazioni del CAD o di ogni altra norma in materia di digitalizzazione ed innovazione della Pubblica Amministrazione e risulta quindi non rientrante nelle funzioni attribuite al Difensore civico per il digitale dall'art. 17 comma 1-quater del CAD. Per tale motivo detta comunicazione si ritiene vada considerata come richiesta di informazioni e non come segnalazione, con conseguente archiviazione della stessa.

Si ritiene, comunque, opportuno fornire di seguito il supporto informativo richiesto sull'argomento in questione.

Al riguardo si fa presente che le misure minime rappresentano un supporto metodologico ed un veicolo attraverso il quale le Amministrazioni, soprattutto quelle di minori dimensioni, possono verificare autonomamente la propria infrastruttura ed avviare un percorso di monitoraggio e miglioramento. In termini pratici, l'applicazione delle misure minime serve a ridurre al minimo i rischi di:

- accessi non autorizzati ai sistemi;
- trattamento di dati non consentiti o non conformi alle normali finalità;
- modifica di dati in conseguenza di interventi non autorizzati o non conformi alle regole;
- distruzione o perdita, anche accidentale, di dati.

Tecnicamente le misure minime sottolineano quelle che dovrebbero essere comuni regole di buon senso (nonché *best practices* internazionalmente riconosciute) nella conduzione ed organizzazione dei sistemi ICT e, di per sé, la loro implementazione non dovrebbe normalmente creare alcun tipo di problema tecnico/organizzativo. Il fatto che alcune amministrazioni utilizzino siti ed accessi non dotati della cifratura di canale tramite i protocolli HTTPS/TLS è una prassi altamente sconsigliata nell'attuale contesto.

Di conseguenza, non si suggerisce di abbassare i controlli minimi di sicurezza in favore di una maggior facilità operativa poiché l'Amministrazione, in caso di incidente informatico dovuto all'inosservanza delle stesse, potrebbe essere chiamata a risponderne direttamente.

Nel caso in cui ci si imbatta in un sito e/o servizio non conforme agli attuali standard di utilizzo sicuro, si invita a comunicare secondo le modalità disponibili al *link* https://www.cert-pa.it/segnalazioni/ le coordinate del servizio stesso, in modo da attuare i passi opportuni per la risoluzione/mitigazione della problematica riscontrata.

Ciò rappresentato, fiduciosi di aver comunque fornito elementi di Suo interesse, Le invio cordiali saluti.

Massimo Macchia