COMMISSIONE
EUROPEA

Bruxelles, 12.9.2018
COM(2018) 637 final

COMUNICAZIONE DELLA COMMISSIONE AL PARLAMENTO EUROPEO, AL CONSIGLIO, AL COMITATO ECONOMICO E SOCIALE EUROPEO E AL COMITATO DELLE REGIONI

Assicurare elezioni europee libere e corrette

Contributo della Commissione europea all'incontro dei leader di Salisburgo del 19-20 settembre 2018

Assicurare elezioni europee libere e corrette

Un momento cruciale per il futuro dell'Unione europea

La difesa della democrazia e dei valori democratici costituiscono l'essenza stessa dell'Unione europea. Si tratta di un imperativo in una società in cui prevalgono pluralismo e tolleranza e in cui i cittadini europei possono votare avendo la certezza di non essere indotti in errore. Assieme allo Stato di diritto e ai diritti fondamentali, la democrazia è parte della nostra identità e definisce la nostra Unione.

Le elezioni del Parlamento europeo del maggio 2019 si terranno in un contesto molto diverso rispetto a tutte le elezioni precedenti. Le sfide politiche per l'Unione e per i suoi Stati membri sono enormi. Vi è la chiara necessità di forgiare un'Unione più forte, che possa agire con credibilità e forza sul palcoscenico mondiale, dove si contendono il potere potenze mondiali che non condividono necessariamente tutti i nostri interessi e i nostri valori. Un'Unione forte, fondata su una cooperazione giudiziaria efficace, sullo scambio di informazioni per lottare contro il terrorismo e la criminalità organizzata e su un mercato interno ben funzionante, richiede fiducia reciproca tra gli Stati membri e nei rispettivi sistemi democratici. In questo contesto unico le elezioni europee del maggio 2019 determineranno il futuro dell'Unione europea nei prossimi anni.

Assicurare la resilienza dei sistemi democratici dell'Unione rientra tra gli scopi dell'Unione della sicurezza: gli attacchi contro le infrastrutture elettorali e i sistemi informatici per le campagne elettorali costituiscono minacce ibride che l'Unione deve affrontare. Le campagne di disinformazione di massa *online* basate su motivazioni politiche, anche attuate da paesi terzi, aventi l'obiettivo specifico di screditare e delegittimare le elezioni, sono state riconosciute come minacce crescenti per le nostre democrazie[1]. L'Unione europea dovrebbe fare tutto quanto in suo potere per difendere i propri processi democratici dalle manipolazioni da parte di paesi terzi o dettate da interessi privati. I periodi elettorali si sono rivelati particolarmente esposti alla disinformazione mirata. Questi attacchi compromettono l'integrità e la correttezza del processo elettorale e minano la fiducia dei cittadini nei loro rappresentanti eletti, mettendo pertanto a rischio la democrazia stessa.

I cittadini europei dovrebbero poter votare avendo pienamente compreso le loro scelte politiche. Ciò richiede una maggiore consapevolezza delle minacce e una maggiore trasparenza dei nostri processi politici. Una sfera pubblica aperta, protetta da influenze indebite, garantisce condizioni di parità per campagne elettorali e per elezioni nelle quali il pubblico possa avere fiducia[2]. Per le nostre democrazie è essenziale creare spazi che consentano una campagna politica dinamica, la quale offra agli elettori un quadro chiaro e non

[1] Cfr. la comunicazione congiunta al Parlamento europeo, al Consiglio europeo e al Consiglio, Rafforzamento della resilienza e potenziamento delle capacità di affrontare minacce ibride (JOIN(2018) 16 final) e le conclusioni del Consiglio europeo del 28 giugno 2018 (http://www.consilium.europa.eu/it/press/press-releases/2018/06/29/20180628-euco-conclusions-final/pdf).

[2] La Commissione di Venezia del Consiglio d'Europa ha formulato orientamenti sulle elezioni (https://www.venice.coe.int/webforms/documents/default.aspx?pdffile=CDL-AD(2002)023rev2-ita), anche per l'ambiente mediatico (http://www.venice.coe.int/webforms/documents/?pdf=CDL-PI(2016)006-e).

distorto delle idee e dei programmi dei partiti che concorrono al voto. Pertanto, le frodi e gli altri tentativi intenzionali di manipolazione delle elezioni dovrebbero essere combattuti attivamente, anche mediante sanzioni.

Le attività *online*, anche durante il processo elettorale, hanno registrato un rapido aumento e pertanto è fondamentale assicurare maggiore sicurezza e condizioni di parità politica. Anche *online* dovrebbero applicarsi le salvaguardie elettorali convenzionali ("*offline*"), quali le norme applicabili alle comunicazioni politiche in periodo elettorale, la trasparenza sulle spese elettorali e le relative limitazioni, il rispetto dei periodi di silenzio elettorale e la parità di trattamento dei candidati[3]. La trasparenza sulla pubblicità politica in televisione o sui cartelloni e i relativi limiti, nonché la trasparenza della pubblicità politica stessa dovrebbero applicarsi anche nel mondo *online*, cosa che non avviene attualmente e a cui occorre porre rimedio prima delle prossime elezioni europee.

Nuove sfide e sviluppi recenti

La comunicazione *online*, che ha ridotto le barriere e i costi sostenuti dai soggetti politici per interagire con i cittadini, offre grandi opportunità, ma ha anche aumentato le possibilità offerte a soggetti malintenzionati di condizionare il dibattito democratico e i processi elettorali. L'ambiente *online* può facilitare la presentazione delle informazioni, nascondendone però l'origine o la finalità, anche celando il fatto che una comunicazione (quale un post sui media sociali) sia in realtà una pubblicità a pagamento e non una comunicazione fattuale, facendo passare per giornalismo quelle che sono semplici opinioni personali e presentando informazioni in modo selettivo per esacerbare le tensioni e polarizzare il dibattito. Nessuno dovrebbe farsi illusioni su tali minacce: l'Unione europea e i suoi sistemi politici non ne sono immuni.

Inoltre, l'integrità delle elezioni può essere seriamente compromessa da incidenti informatici "convenzionali", compresi gli attacchi informatici contro i processi elettorali, le campagne elettorali, le infrastrutture dei partiti politici, i sistemi dei candidati o delle autorità pubbliche e l'uso improprio dei dati personali. Le recenti rivelazioni, tra l'altro sul caso "Facebook/Cambridge Analytica", ne sono un tipico esempio. Si pensa che i dati personali siano stati impropriamente utilizzati e forniti illegalmente a terzi per usi molto diversi da quelli originariamente previsti. Il caso ha messo in luce il potenziale rischio che alcune attività *online* siano utilizzate per fare dei cittadini il bersaglio di pubblicità e di comunicazioni politiche occulte, trattando illecitamente e utilizzando abusivamente i loro dati personali per

[3] Cfr. la recente pubblicazione del Consiglio d'Europa dal titolo "*Internet and electoral campaigns – Study on the use of internet in electoral campaigns*" (Internet e le campagne elettorali – Studio sull'uso di internet nelle campagne elettorali) frutto del lavoro del comitato di esperti sul pluralismo dei media e la trasparenza della proprietà dei media (MSI-MED) del Consiglio d'Europa (https://www.coe.int/en/web/human-rights-rule-of-law/-/internet-and-electoral-campaigns-a-new-study-has-been-published). Lo studio esamina le implicazioni dello spostamento su internet della pubblicità elettorale, in particolare per quanto riguarda le spese elettorali e le tecniche pubblicitarie basate sul *micro-targeting* degli elettori con messaggi personalizzati. Cfr. anche la raccomandazione CM/Rec (2016) 5 del Consiglio d'Europa sulla libertà di internet, che richiama la responsabilità dei governi, delle piattaforme e degli intermediari per le campagne politiche condotte *online* dai partiti politici, dai candidati e da altri soggetti.

manipolare le opinioni, diffondere disinformazione o semplicemente distorcere la verità a favore di determinati obiettivi politici o per fomentare divisioni[4].

Sostenere elezioni libere e corrette in Europa

Non è compito delle istituzioni europee organizzare le elezioni, che rimangono principalmente di competenza degli Stati membri. Gli Stati membri sono responsabili dell'organizzazione delle elezioni e del controllo dello svolgimento del processo elettorale[5]. Vi è, tuttavia, un'evidente dimensione unionale. In quanto presentano candidati alle elezioni del Parlamento europeo, i partiti politici nazionali e regionali sono tra i principali artefici delle campagne elettorali europee. I partiti politici europei e le fondazioni ad essi associate hanno una funzione importante nell'organizzazione di campagne complementari a livello europeo, anche per i candidati capilista alla carica di presidente della Commissione europea.

Dopo le elezioni del Parlamento europeo del 2014, nella sua relazione post-elezioni del 2015[6], la Commissione si è impegnata a definire metodi per accrescere ulteriormente la dimensione europea e per rafforzare la legittimità democratica del processo decisionale dell'Unione, nonché a esaminare ulteriormente e a cercare di risolvere le cause della persistente bassa affluenza alle urne in alcuni Stati Membri. Nel febbraio 2018 la Commissione ha invitato ad avviare un dialogo tempestivo e continuo con i cittadini sulle questioni europee, a dare un inizio anticipato alla campagna elettorale dei partiti politici per le elezioni del Parlamento europeo, tra cui quelle dei rispettivi candidati alla carica di presidente della Commissione europea, ha chiesto una maggiore trasparenza sui legami tra partiti politici nazionali ed europei e ha esortato gli Stati membri a promuovere il diritto di voto, in particolare dei gruppi sottorappresentati.

L'Unione europea ha anche già adottato misure importanti per rafforzare la resilienza democratica in Europa, anche con il nuovo quadro europeo per la protezione dei dati in vigore dal maggio di quest'anno. Il regolamento generale sulla protezione dei dati, ormai in applicazione in tutta l'Unione europea, fornisce gli strumenti necessari per affrontare i casi di uso illecito dei dati personali nel contesto elettorale. Sono inoltre in corso lavori per promuovere un ambiente *online* più sicuro, rafforzando la nostra resilienza complessiva alle

[4] Cfr. la relazione intermedia pubblicata dall'autorità britannica per la protezione dei dati del Regno Unito (ICO) sull'indagine formale avviata sull'uso delle tecniche di analisi dei dati a fini politici a seguito dei sospetti di trattamento illecito dei dati e *micro-targeting* di annunci politici durante la campagna per il referendum UE (https://ico.org.uk/media/action-weve-taken/2259371/investigation-into-data-analytics-for-political-purposes-update.pdf). Come sottolinea la relazione, la rapidità dell'evoluzione sociale e tecnologica dell'uso dei megadati (*big data*) ha fatto sì che vi sia una conoscenza limitata, o una scarsa trasparenza, sulle tecniche di trattamento dei dati utilizzate "dietro le quinte" (compresi gli algoritmi, le analisi, l'abbinamento di dati e la profilazione) dalle organizzazioni e dalle imprese per prendere di mira le singole persone. È chiaro che questi strumenti possono avere un impatto significativo sulla vita privata delle persone. È importante che vi sia una maggiore e reale trasparenza sull'uso di tali tecniche per assicurare che le persone abbiano il controllo dei propri dati personali e che la legge sia rispettata. Quando la finalità dell'uso di dette tecniche è legata al processo democratico, l'esigenza di standard elevati di trasparenza è molto forte. La relazione sottolinea anche l'importanza di integrare meglio le considerazioni in materia di protezione dei dati nel più ampio quadro normativo di disciplina delle elezioni.

[5] A norma del diritto dell'UE e nel rispetto dei loro obblighi internazionali.

[6] Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni - Relazione sulle elezioni del Parlamento europeo del 2014 (COM(2015)206 final).

minacce informatiche, tra cui la disinformazione *online* e la manipolazione dei comportamenti.

È importante fare la massima chiarezza sulle modalità di attuazione in questo contesto delle norme europee in materia di protezione dei dati, e occorre anche intensificare gli sforzi per accrescere la consapevolezza, aumentare la trasparenza e rafforzare la sicurezza. I cittadini dovrebbero essere in grado di sapere da chi provengono la pubblicità e i messaggi politici *online* che ricevono e chi li finanzia. Gli orientamenti sulle modalità di attuazione, nel quadro delle elezioni europee, delle nuove norme sulla protezione dei dati dovrebbero contribuire a una maggiore chiarezza e a una migliore comprensione, visto che la maggiore cooperazione e lo scambio di informazioni tra le autorità competenti e con altri soggetti contribuiscono ad accrescere la sicurezza.

Il pacchetto per rafforzare la resilienza democratica presentato insieme alla presente comunicazione comprende azioni equilibrate, globali e mirate a sostegno dell'integrità e dell'efficace svolgimento delle elezioni del Parlamento europeo del 2019. Si tratta di una responsabilità congiunta di tutti i soggetti coinvolti nel processo elettorale. Richiede una vigilanza costante e un adattamento flessibile ad un ambiente dinamico e ai nuovi sviluppi tecnologici. Formulando orientamenti e raccomandazioni e fornendo gli strumenti necessari si consentirà ai partiti politici europei e nazionali, ai governi nazionali, alle autorità, ai privati e ai portatori di interesse di collaborare con maggiore chiarezza per creare un ambiente democratico più sicuro e condizioni di parità.

Gli Stati membri sono invitati ad applicare i predetti principi anche ad altre elezioni e referendum organizzati a livello nazionale.

Le misure proposte con il presente pacchetto mirano a:

1. fornire orientamenti specifici in merito al trattamento dei dati personali nel contesto delle elezioni;
2. raccomandare le migliori pratiche per affrontare i rischi di disinformazione e gli attacchi informatici e per promuovere la trasparenza e la responsabilità nel processo elettorale dell'UE; rafforzare la cooperazione tra le autorità competenti e mettere in atto gli strumenti che consentano loro di intervenire e, se del caso, prevedere sanzioni per salvaguardare l'integrità del processo elettorale;
3. contrastare i casi in cui i partiti politici o le fondazioni ad essi associate si avvalgono di pratiche che violano le norme in materia di protezione dei dati per influenzare o tentare di influenzare deliberatamente il risultato delle elezioni europee.

Con questo pacchetto la Commissione ha cercato di evitare gli oneri amministrativi inutili e ha avuto cura di evitare di limitare indebitamente il margine di manovra dei partiti politici europei, regionali e nazionali e delle relative fondazioni.

1. I vigenti strumenti dell'UE di tutela di elezioni libere e corrette

L'Unione ha già adottato misure importanti per tutelare l'integrità delle elezioni e rafforzare il processo democratico.

Con il regolamento generale sulla protezione dei dati[7], che ha trovato applicazione diretta in tutta l'Unione a decorrere dal 25 maggio 2018, l'Unione europea ha ora tutti gli strumenti per contribuire a prevenire e ad affrontare l'uso illecito dei dati personali. In tal modo l'Unione europea ha fatto scuola in questo ambito.

Inoltre, recentemente è stato modificato l'atto relativo all'elezione dei membri del Parlamento europeo, anche per garantire una maggiore trasparenza del processo elettorale europeo[8]. La revisione del regolamento relativo allo statuto e il finanziamento dei partiti politici europei[9], adottata il 3 maggio 2018, migliora il riconoscimento, l'efficacia, la trasparenza e la responsabilità dei partiti politici europei e delle fondazioni politiche europee. La raccomandazione (UE) 2018/234 della Commissione[10] evidenzia le tappe principali per rafforzare ulteriormente l'efficienza nello svolgimento delle elezioni del Parlamento europeo del 2019.

La direttiva 2002/58/CE del Parlamento europeo e del Consiglio[11] (direttiva relativa alla vita privata e alle comunicazioni elettroniche) si applica alle comunicazioni indesiderate a scopo di commercializzazione diretta, compresi i messaggi politici trasmessi dai partiti politici e da altri soggetti coinvolti nel processo elettorale. La direttiva garantisce inoltre la riservatezza e tutela le informazioni archiviate nelle apparecchiature terminali degli utenti, come smartphone o computer[12]. La proposta di regolamento sulla vita privata e le comunicazioni elettroniche[13], attualmente in fase di negoziazione, rafforzerà ulteriormente il controllo dei cittadini grazie all'accresciuta trasparenza e amplierà l'ambito di applicazione della protezione oltre i tradizionali operatori di telecomunicazione includendo i servizi di comunicazione elettronica basati su internet.

---

[7] Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati) (GU L 119 del 4.5.2016, pag. 1).

[8] Decisione (UE, Euratom) 2018/994 del Consiglio, del 13 luglio 2018, che modifica l'atto relativo all'elezione dei membri del Parlamento europeo a suffragio universale diretto, allegato alla decisione 76/787/CECA, CEE, Euratom del 20 settembre 1976 (https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:32018D0994&qid=1531826494620).

[9] Regolamento (UE, Euratom) n. 1141/2014 del Parlamento europeo e del Consiglio, del 22 ottobre 2014, relativo allo statuto e al finanziamento dei partiti politici europei e delle fondazioni politiche europee (GU L 317 del 4.11.2014, pag. 1).

[10] Raccomandazione (UE) 2018/234 della Commissione, del 14 febbraio 2018, sul rafforzare la natura europea e l'efficienza nello svolgimento delle elezioni del Parlamento europeo del 2019 (GU L 45 del 17.2.2018, pag. 40).

[11] Direttiva 2002/58/CE del Parlamento europeo e del Consiglio, del 12 luglio 2002, relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche (direttiva relativa alla vita privata e alle comunicazioni elettroniche) (GU L 201 del 31.7.2002, pag. 37).

[12] Per accedere a dette informazioni o per tenere traccia del comportamento *online* degli utenti, ad esempio salvando *cookie* sui loro dispositivi, i siti web devono acquisire il consenso degli utenti.

[13] Proposta di regolamento del Parlamento europeo e del Consiglio relativo al rispetto della vita privata e alla tutela dei dati personali nelle comunicazioni elettroniche e che abroga la direttiva 2002/58/CE (regolamento sulla vita privata e le comunicazioni elettroniche) (COM(2017) 10 final).

Inoltre, recentemente, nella sua comunicazione del 26 aprile 2018[14], la Commissione ha presentato un approccio europeo per lottare contro la disinformazione *online*. Con la comunicazione la Commissione intende promuovere un ambiente *online* più trasparente, più affidabile e più responsabile. Tra gli obiettivi principali vi è lo sviluppo di un ambizioso **codice di buone pratiche sulla disinformazione**, che dovrebbe, in particolare, prevedere l'impegno delle piattaforme *online* e del settore della pubblicità a garantire la trasparenza e a limitare le possibilità di praticare la pubblicità politica mirata[15]. Il codice, la cui pubblicazione è prevista per il settembre 2018[16], dovrebbe produrre risultati misurabili entro ottobre.

Più specificamente, i firmatari del codice di buone pratiche dovrebbero accettare di privare di entrate pubblicitarie i siti web "impostori" e i siti web che pubblicano disinformazione, dovrebbero garantire la trasparenza sui contenuti sponsorizzati, in particolare nella pubblicità politica e nella pubblicità su questioni etiche, dovrebbero istituire sistemi di marcatura chiari e introdurre regole sui *bot*[17], che assicurino che le attività di questi ultimi non possano essere confuse con un'interazione con esseri umani, e dovrebbero intensificare gli sforzi per chiudere gli *account* fasulli. I firmatari dovrebbero inoltre accettare di agevolare la valutazione dei contenuti da parte degli utenti, incoraggiando lo sviluppo di indicatori di affidabilità delle fonti, dovrebbero ridurre la visibilità della disinformazione migliorando la reperibilità dei contenuti affidabili e dovrebbero fornire agli utenti informazioni sul modo in cui gli algoritmi attribuiscono il grado di priorità ai contenuti. Inoltre, i firmatari dovrebbero fornire l'accesso ai dati della piattaforma ad organismi affidabili di verifica dei fatti e agli studiosi. Una valutazione del codice di buone pratiche sarà effettuata nel quadro dell'elaborazione di un piano di azione con proposte specifiche per una risposta coordinata dell'UE alla sfida della disinformazione, che sarà presentato dalla Commissione e dall'Alto rappresentante prima della fine dell'anno.

Per quanto riguarda gli incidenti informatici più "tradizionali", come la pirateria contro i sistemi informatici o il defacciamento dei siti web, a livello UE la direttiva 2013/40/UE ha armonizzato le definizioni dei reati e i livelli massimi minimi delle sanzioni per gli attacchi contro i sistemi di informazione.

Il gruppo di cooperazione istituito dalla direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio[18] ha indicato come sfida comune la cibersicurezza delle elezioni. Il gruppo di cooperazione, che comprende le autorità nazionali competenti per la cibersicurezza, la Commissione e l'Agenzia dell'Unione europea per la sicurezza delle reti e dell'informazione

[14] Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni - Contrastare la disinformazione *online*: un approccio europeo (COM(2018) 236 final).
[15] Per l'elaborazione del codice di buone pratiche, nel maggio 2018 la Commissione ha istituito un forum, costituito da un "gruppo di lavoro" (composto dalle principali piattaforme *online* e dai rappresentanti del settore pubblicitario e dei principali inserzionisti) e da un gruppo avente funzione di "cassa di risonanza" (composto da rappresentanti dei media e della società civile).
[16] Dopo che il gruppo avente funzione di "cassa di risonanza" avrà emesso il suo parere.
[17] Con il termine *bot* si indicano l'inserimento automatico di post sulle piattaforme di media sociali, ma anche applicazioni più interattive, ad esempio i *chatbot*, che interagiscono direttamente con gli utenti.
[18] Direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio, del 6 luglio 2016, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione (GU L 194 del 19.7.2016, pag. 1).

(ENISA) ha inventariato le iniziative nazionali esistenti in materia di cibersicurezza delle reti e dei sistemi informativi utilizzati per le elezioni. Ha individuato i rischi associati ad un livello insufficiente di cibersicurezza che potrebbero incidere sulle prossime elezioni del Parlamento europeo e, sulla base delle esperienze e delle migliori prassi, ha elaborato un compendio sulla cibersicurezza delle tecnologie elettorali, comprese misure tecniche e organizzative. Il compendio fornisce una guida pratica per le autorità competenti in materia di cibersicurezza e per gli organismi di gestione delle elezioni.

2. Rafforzare ulteriormente la resilienza democratica: potenziare ulteriormente le reti di cooperazione, la trasparenza *online*, la protezione dagli incidenti di cibersicurezza e la lotta contro le campagne di disinformazione nel contesto delle elezioni del Parlamento europeo

Data l'entità della sfida e visto che le responsabilità formali in questo ambito sono condivise tra più autorità, sarà possibile conseguire risultati significativi solo grazie alla collaborazione tra tutti i soggetti interessati.

La presente comunicazione è accompagnata da una raccomandazione relativa alle reti di cooperazione in materia elettorale, alla trasparenza *online*, alla protezione dagli incidenti di cibersicurezza e alla lotta contro le campagne di disinformazione nel contesto delle elezioni del Parlamento europeo. Per garantire lo svolgimento di elezioni libere e corrette, la presente raccomandazione dovrebbe essere attuata da tutti i soggetti in tempo utile per le elezioni del Parlamento europeo del 2019.

La raccomandazione incoraggia ciascuno Stato membro a istituire e sostenere una rete nazionale per le questioni elettorali. Le autorità degli Stati membri competenti in materia elettorale dovrebbero cooperare in modo rapido ed efficace con le autorità competenti in settori connessi (quali le autorità per la protezione dei dati, le autorità di regolamentazione dei media, le autorità per la cibersicurezza, ecc.) e, se necessario, anche con le autorità di contrasto. In tal modo potranno individuare rapidamente potenziali minacce per le elezioni del Parlamento europeo e intervenire rapidamente per far rispettare le norme vigenti, comprese le sanzioni finanziarie previste, quali la restituzione del contributo pubblico. La normativa dell'UE e nazionale deve essere rispettata e fatta rispettare. In questa prospettiva, la Commissione invita gli Stati membri a promuovere, a norma del diritto applicabile, nazionale e dell'Unione, la condivisione delle informazioni tra le autorità per la protezione dei dati e le autorità incaricate del monitoraggio delle elezioni e delle attività e del finanziamento dei partiti politici, qualora dalle loro decisioni consegua, o vi siano altrimenti ragionevoli motivi di ritenere, che la violazione sia legata ad attività politiche dei partiti politici nazionali o delle fondazioni politiche nazionali nel contesto delle elezioni del Parlamento europeo.

Si raccomanda inoltre agli Stati membri di designare punti di contatto che partecipino ad una rete di cooperazione europea ai fini delle elezioni del Parlamento europeo. La Commissione sosterrà le reti di cooperazione organizzando una prima riunione dei punti di contatto

designati entro gennaio 2019. Nel rispetto delle competenze nazionali e dei requisiti procedurali applicabili alle autorità interessate, detto forum costituirà il nucleo di una procedura di allarme europea in tempo reale e di un forum per lo scambio di informazioni e pratiche tra le autorità degli Stati membri.

I partiti politici, le fondazioni politiche e gli organizzatori delle campagne politiche devono assicurare trasparenza nelle loro comunicazioni politiche ai cittadini e garantire che il processo elettorale europeo non sia distorto da pratiche sleali. La Commissione presenta misure concrete per rafforzare la trasparenza, in modo che i cittadini possano vedere chi si cela dietro la comunicazione politica che ricevono e chi la paga[19]. Gli Stati membri dovrebbero sostenere e agevolare tale trasparenza e gli sforzi delle autorità competenti di monitoraggio delle violazioni e di controllo del rispetto delle norme, anche mediante l'applicazione di sanzioni ove necessario. Se del caso, dovrebbero essere coinvolte anche le autorità di contrasto, per garantire una risposta adeguata agli incidenti e l'applicazione di sanzioni appropriate[20].

La resilienza, la deterrenza e la difesa sono essenziali per creare una cibersicurezza forte per l'Unione europea[21]. Le competenti autorità europee e nazionali, i partiti politici, le fondazioni politiche e gli organizzatori delle campagne politiche dovrebbero essere pienamente consapevoli dei rischi per le elezioni del prossimo anno e dovrebbero adoperarsi con l'impegno dovuto per proteggere la loro rete e i loro sistemi di informazione[22].

[19] Queste proposte sono complementari al codice di buone pratiche in corso di elaborazione da parte del forum multipartecipativo convocato dalla Commissione a seguito della comunicazione del 26 aprile 2018 sulla disinformazione *online*.

[20] Esse riguardano in particolare i casi in cui il processo elettorale è preso di mira con intento illecito, ivi compresi gli incidenti dovuti ad attacchi contro i sistemi di informazione. A seconda delle circostanze, possono risultare necessarie indagini penali che possono sfociare in sanzioni penali. Come osservato in precedenza, la direttiva 2013/40/UE ha armonizzato le definizioni dei reati e dei livelli massimi minimi delle sanzioni per gli attacchi contro i sistemi di informazione.

[21] La comunicazione congiunta dell'Alto rappresentante dell'Unione per gli Affari esteri e la politica di sicurezza e la Commissione europea del settembre 2017 riconosce la necessità di una risposta globale per assicurare una cibersicurezza forte per l'Unione, basata sulla resilienza, sulla deterrenza e sulla difesa (JOIN(2017) 450 final).

[22] Il compendio elaborato dal gruppo di cooperazione istituito dalla direttiva (UE) 2016/1148 fornisce utili orientamenti al riguardo. La direttiva (UE) 2016/1148 mira a conseguire un elevato livello comune di resilienza della cibersicurezza in tutta l'Unione. Per conseguire questo obiettivo, la direttiva sostiene lo sviluppo di capacità nazionali in materia di cibersicurezza e tutela la fornitura di servizi essenziali in settori chiave. Per intensificare gli sforzi per una corretta attuazione della direttiva, fino al 2020 la Commissione offre finanziamenti per oltre 50 milioni di EUR mediante il Meccanismo per collegare l'Europa (CEF). Le misure di gestione dei rischi previste dalla direttiva (UE) 2016/1148 sono punti di riferimento pertinenti per il processo elettorale. Il regolamento generale sulla protezione dei dati prevede inoltre l'obbligo di attuare misure tecniche e organizzative adeguate per garantire la sicurezza dei dati personali trattati. Esso si applica a tutti i soggetti coinvolti nel processo elettorale e prevede inoltre l'obbligo di comunicazione delle violazioni dei dati personali alle autorità competenti per la protezione dei dati e alle persone interessate (cfr. orientamenti della Commissione).

3. Applicare le norme sulla protezione dei dati nel processo elettorale

Il regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio (regolamento generale sulla protezione dei dati)[23], entrato direttamente in applicazione in tutta l'Unione il 25 maggio 2018, fornisce all'Unione gli strumenti necessari per affrontare i casi di uso illecito dei dati personali nel contesto elettorale.

Trattandosi della prima volta in assoluto che dette norme saranno applicate nel contesto elettorale europeo in occasione delle prossime elezioni del Parlamento europeo, è importante che tutti i soggetti coinvolti nel processo elettorale, ossia le autorità elettorali nazionali, i partiti politici, gli intermediari e gli analisti di dati, le piattaforme dei media sociali e le reti pubblicitarie *online*, abbiano chiaro come applicare tali norme nel modo migliore e che cosa esse non consentono.

La Commissione ha pertanto elaborato orientamenti specifici che evidenziano gli obblighi di protezione dei dati pertinenti nel contesto elettorale. Per lottare contro i tentativi illeciti di abuso dei dati personali delle persone, in particolare a fini di *micro-targeting*, le autorità nazionali per la protezione dei dati, in quanto autorità incaricate di far rispettare il regolamento generale sulla protezione dei dati, devono esercitare pienamente i maggiori poteri loro attribuiti per reagire a possibili violazioni.

4. Rafforzare le norme sul finanziamento dei partiti politici europei

I partiti politici e le fondazioni politiche sono naturalmente i principali protagonisti delle elezioni. Attraverso le loro campagne, essi si contendono il voto degli elettori. Per assicurare condizioni di parità politica e per tutelare tutti i partiti politici e tutte le fondazioni politiche da condotte illecite è essenziale prevenire situazioni nelle quali i partiti possano trarre vantaggio da pratiche illegali che violano le norme in materia di protezione dei dati. Sanzioni dovrebbero essere inflitte a coloro che non solo violano la vita privata delle persone, ma che possono anche influire sull'esito delle elezioni del Parlamento europeo. Parallelamente all'invito agli Stati membri ad applicare, ove opportuno, tali sanzioni ai partiti e alle fondazioni a livello nazionale, la Commissione propone di introdurre una modifica mirata del regolamento (UE, Euratom) n. 1141/2014 al fine di prevedere sanzioni proporzionate nei casi che coinvolgono i partiti politici e le fondazioni politiche a livello europeo. Tale modifica, che rafforza le norme vigenti, mira a garantire che le elezioni del Parlamento europeo si svolgano secondo rigorose regole democratiche e nel pieno rispetto dei valori su cui l'Unione si fonda, in particolare la democrazia, i diritti fondamentali e lo Stato di diritto.

[23] Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati) (GU L 119 del 4.5.2016, pag. 1).

La Commissione esorta il Parlamento europeo e il Consiglio a garantire che le modifiche mirate siano messe in atto prima delle elezioni del Parlamento europeo del 2019.

5. Conclusioni

Eventi recenti hanno dimostrato l'esistenza e la gravità dei rischi di manipolazione del processo elettorale, sia mediante attacchi ai sistemi di informazione che mediante l'abuso dei dati personali e il ricorso a pratiche opache. L'UE non ne è immune. Le attività *online* nel contesto elettorale rappresentano una nuova minaccia e richiedono una protezione specifica. Preparandoci ora offriremo un servizio ai cittadini e alla democrazia. Non possiamo attendere l'indomani delle elezioni e dei referendum per scoprirlo e per dare solo allora una risposta.

La protezione della democrazia nell'Unione è una responsabilità condivisa e solenne dell'Unione europea e dei suoi Stati membri. Si tratta inoltre di una questione urgente. Tutti i soggetti coinvolti devono intensificare gli sforzi e collaborare per scoraggiare, prevenire e sanzionare le interferenze illecite nel sistema elettorale. Le misure proposte dalla Commissione in questo pacchetto sostengono questi sforzi.

Dopo le elezioni del Parlamento europeo del 2019 la Commissione riferirà sull'attuazione del presente pacchetto di misure.

Le prossime tappe in vista delle elezioni del Parlamento europeo del 2019

- *La Commissione invita il Parlamento europeo e il Consiglio a garantire che la proposta di modifiche mirate del regolamento (UE) n. 1141/2014 sia messa in atto in tempo per le elezioni del Parlamento europeo del 2019.*

- *Insieme all'Alto rappresentante, la Commissione sosterrà la preparazione di una risposta europea comune a ogni coinvolgimento straniero nelle elezioni nell'Unione europea[24]. Dando seguito alle conclusioni del Consiglio europeo del giugno 2018 e in collaborazione con gli Stati membri, essi presenteranno, entro dicembre 2018, un piano di azione con proposte specifiche per una risposta coordinata dell'UE alla sfida della disinformazione.*

- *La Commissione intende fare opera di sensibilizzazione e mantenere aperto il dialogo con le autorità degli Stati membri mediante la conferenza ad alto livello del 15 e 16 ottobre 2018 sulle minacce alle elezioni basate sull'uso di strumenti informatici, i cui risultati confluiranno nel prossimo convegno sui diritti fondamentali (26 e 27 novembre 2018), incentrato sulla "Democrazia nell'Unione europea".*

[24] Potrebbe anche essere previsto l'uso delle misure elaborate in attuazione del quadro relativo ad una risposta diplomatica comune dell'UE alle attività informatiche dolose.