Les enjeux politiques et juridiques de la sécurité informatique et technologique dans le processus électoral roumain

§.1. Introduction

Je suis honoré et heureux de participer et parler devant pareil aréopage sûr un thème qui soulève des questions qui sont au cœur de toutes nos préoccupations. Il s'agit de questions qui découlent des contradictions mêmes entre la nature ouverte des élections et les subtilités inhérentes à la technologie moderne. Il implique la légitimité et l'efficacité des politiques publiques relatives à la gestion des élections, il ouvre des questions sur les options pour développer les processus électoraux modernes et il traite de la relation entre la confiance dans la technologie moderne et la confiance dans les élections.

Mon présentation propose une esquisse du concept de sécurité informatique et de sa relation avec le droit électoral et les processus électoraux en Roumanie, la cyber-sécurité représentant selon le contexte, soit un frein à l'informatisation électorale, soit un catalyseur de la réforme électorale.

Le concept de sécurité informatique a une dimension normative, établie à travers *La stratégie de cyber-sécurité de la Roumanie*, approuvée par décision gouvernementale.

La sécurité informatique représente le statut de normalité résultant de l'application d'un ensemble de mesures proactives et réactives qui assurent la confidentialité[1], l'intégrité[2], la disponibilité[3], l'authenticité[4] et la non-répudiation[5] de

[1] Confidentialité – pour assurer l'accès aux informations classifiées uniquement sur la base de l'habilitation de sécurité, en conformité avec le niveau de confidentialité des informations consultées et l'autorisation résultant de l'application du principe du besoin de savoir/need to know.

[2] Intégrité – pour interdire de changer – par la suppression ou l'ajout - ou par la destruction sans autorisation des informations classifiées.

[3] Disponibilité – pour assurer les conditions nécessaires à la facilitation de la recherche et de l'utilisation des informations classifiées, chaque fois que nécessaire, dans le strict respect de ses conditions de confidentialité et d'intégrité.

[4] Authenticité - pour s'assurer de l'authenticité de toutes les données, transactions, communications (en format électronique ou physique). En outre, il est important que les identités des deux parties impliquées soient confirmées.

[5] Non-répudiation - mesure visant à garantir qu'après l'émission/réception des informations dans un système de communication sécurisé, l'expéditeur/bénéficiaire ne puisse nier à tort, qu'il a envoyé/reçu l'information.

l'information électronique, des les ressources et services publics ou privés dans l'espace cybernétique.[6]

Les mesures proactives et réactives peuvent inclure des concepts, normes et directives pour la sécurité qui mettent en œuvre des solutions d'ingénierie pour protéger l'infrastructure cybernétique, la gestion de l'identité et la gestion des conséquences.[7]

Le concept de sécurité informatique est essentiellement corrélé aux notions de cyberdéfense et de cyber-menace.

La cyberdéfense peut être décrite comme l'ensemble des mesures prises dans le l'espace cybernétique pour protéger, surveiller, détecter, contrer l'agression et assurer une réponse appropriée contre des menaces cybernétiques spécifiques à l'infrastructure de défense nationale.

Les menaces émanant de l'espace cybernétique se matérialisent- en exploitant les vulnérabilités de nature humaine, technique et procédurale - le plus souvent sous la forme de:

- les cyberattaques contre les infrastructures supportant des fonctions de nature publique ou des services de la société de l'information, dont la perturbation ou l'endommagement pourraient constituer un danger pour la sécurité nationale;
- l'accès non autorisé aux infrastructures cybernétiques;
- modification, suppression ou détérioration de données informatiques ou restriction illégale et non autorisée de l'accès à ces données;
- cyber espionnage.

Selon *La Stratégie de cybersécurité de l'Union européenne: un cyberespace ouvert, sûr et sécurisé, par sécurité informatique on entend généralement les mesures de sauvegarde et les actions auxquelles il est possible de recourir pour protéger le cyberespace, dans les domaines civil et militaire, des menaces associées à ses réseaux interdépendants et à son infrastructure informatique ou susceptibles de leur porter atteinte. La cybersécurité vise à préserver la disponibilité et l'intégrité des réseaux et de l'infrastructure ainsi que la confidentialité des informations qui y sont contenues*.[8]

[6] La stratégie de cyber-sécurité de la Roumanie approuvée par la Décision gouvernementale n° 271/2013 ;
[7] Ibidem;
[8] http://eeas.europa.eu/archives/docs/policies/eu-cyber-security/cybsec_comm_fr.pdf;

La cybersécurité pourrait également être perçue comme une caractéristique clé de la qualité des processus et systèmes informatiques, sans laquelle l'efficacité est impossible.[9]

De manière pragmatique, le concept de cybersécurité peut être équivalent à l'expression «absence de danger» et le concept d '«insécurité» à «présence de danger». Par conséquence, une haute sécurité correspond à un faible danger et une faible sécurité à un danger élevé.[10]

Une autre façon d'analyser la cybersécurité est liée à ses trois éléments fondamentaux: la protection, la prudence et le traitement de l'événement indésirable.[11]

En tant que processus cybernétique, la cybersécurité a sa propre voie, un objectif précis à suivre - la stabilité, une législation spécifique, un support technologique approprié, basé sur des stratégies, normes, méthodologies, technologies, processus et institutions spécialisées capables d'assurer les services de sécurité, de protection, de fiabilité, de surveillance mais aussi les conditions de disponibilité et de pérennité des systèmes et de leurs utilisateurs.[12]

Dans le processus électoral, la cybersécurité acquiert une dimension spécifique et variable, bordée par les interactions entre le processus électoral et les nouvelles technologies, ou mieux, par le champ d'action de la technologie de l'information sur le marché électoral.

L'utilisation des infrastructures informatiques et d'Internet dans le processus électoral en Roumanie a modifié de façon irréversible le droit électoral national, offrant des promesses d'accroître l'intégrité électorale et créant une dépendance tant pour les administrateurs du processus que pour ses acteurs sous la domination de gros vendeurs. Elle a provoqué des tensions parmi les acteurs politiques concernant l'utilisation de la technologie informatique pour favoriser l'accès au processus électoral et elle a révélé des vulnérabilités organisationnelles tout en générant un nouvel ensemble de risques et de menaces à l'équité des élections.

[9] https://studiidesecuritate.wordpress.com/2011/08/11/evolutia-conceptelor-de-securitate/;
[10] Ibidem;
[11] Ibidem;
[12] Ibidem.

En outre, les nouvelles technologies exercent une pression constante sur le droit électoral roumain à travers la diversification de ses sources formelles et leur surspécialisation, dans le but d'accroître son efficacité et flexibilité en corrélation avec les évolutions rapides de la technologie de l'information.

À partir de 2015, les dispositions normatives sur l'utilisation des technologies de l'information dans les élections se trouvent dans des lois, des décisions gouvernementales, les décisions, les instructions et les directives de l'Autorité électorale permanente, les décisions et les circulaires du Bureau électoral central.

Les points de rencontre de la technologie de l'information avec les processus électoraux en Roumanie se trouvent dans les suivantes étapes du processus électoral:

- Registration des électeurs;
- La vérification de l'éligibilité des électeurs;
- La centralisation des résultats et la répartition des sièges.

§.2. Registration des électeurs

L'inscription des électeurs se fait à travers le Registre électoral, un système informatique national utilisant le réseau internet pour l'enregistrement et la mise à jour des données d'identification des citoyens roumains disposant du droit de vote et des informations concernant leur affectation aux bureaux de vote.

Le registre électoral a été intègre dans la législation organique sur les élections législatives de 2008, avec le but d'être mis en œuvre à partir des élections législatives de 2012, sans aucune étude de faisabilité ou technique, le préalable absolument nécessaire du point de vue des normes des techniques législatives roumaines.

Inévitable, le décalage entre la loi et la pratique a empêché la mise en œuvre aux élections de 2012, l'entrée en vigueur des dispositions légales réglementant l'organisation et son fonctionnement étant reportée au 1er janvier 2013.

Par la suite, en juillet-août 2013, l'Autorité électorale permanente a mené à bien un test national du Registre électoral qui a fourni un certain nombre d'enseignements sous-tendant un nouvel acte normatif primaire qui a constitué la base du fonctionnement efficace du Registre électoral pour les élections de Parlement européen et pour les présidentielles roumaines en 2014.

L'évolution de la dimension normative du système informatique ne s'est pas arrêtée ici. En 2015, une réforme normative complète a été mise en place et cela a introduit, pour la première fois, des règles claires concernant la sécurité du registre électoral.

À compter de 2015, l'Autorité électorale permanente élabore et adopte des instructions concernant les mesures de sécurité relatives à l'administration et à l'utilisation du registre électoral concernant:[13]

- le contrôle de l'accès à l'équipement et au système informatique, afin d'empêcher l'accès par des personnes non autorisées à l'équipement utilisé pour mener des opérations dans le registre électoral;

- le contrôle du support de données, afin d'empêcher la lecture, la copie, la modification ou l'effacement non autorisés du support de données;

- le contrôle du stockage, afin d'empêcher la saisie non autorisée de données et l'inspection, la modification ou l'effacement non autorisés de données;

- le contrôle de l'utilisation, afin d'empêcher l'utilisation de systèmes automatisés de traitement de données par des personnes non autorisées à l'aide d'un équipement de transmission de données;

- le contrôle d'accès aux données, afin de limiter l'accès des personnes autorisées à utiliser le Registre électoral uniquement aux données pour lesquelles elles ont été autorisées;

- le contrôle des entrées de données, afin d'assurer une vérification et une identification ultérieures des données introduites dans le Registre électoral, quand et par qui elles ont été introduites;

- le contrôle du transport et transfert de données, afin d'empêcher la lecture, la copie, la modification ou l'effacement non autorisés de données pendant leur transmission ou pendant le transport de support de données, en garantissant des mesures techniques;

[13] Loi n° 208/2015 concernant l'élection du Sénat et de la Chambre des Députés, ainsi que portant sur l'organisation et le fonctionnement de l'Autorité électorale permanente.

- le contrôle des communications spécifiques au registre électoral, afin d'assurer la vérification et l'identification des autorités/organismes qui ont reçu ou peuvent recevoir des données personnelles, en utilisant des équipements de communication.

Afin de remplir ses pouvoirs relatifs à l'administration et au soutien technique nécessaires au fonctionnement du registre électoral, à la coordination et à l'orientation méthodologique des personnes autorisées à opérer dans le registre électoral, ainsi qu'au contrôle du respect des dispositions légales applicables dans ce domaine, l'Autorité électorale permanente adopte des mesures techniques, opérationnelles et procédurales, selon les principes suivants:

- la confidentialité - fournir un accès à l'information uniquement aux personnes autorisées en fonction de leurs compétences;

- l'intégrité - assurer la nature exacte et complète de l'information, ainsi que les méthodes de traitement;

- la disponibilité – assurer l'accès à l'information dans la limité des délais requis;

- l'identification et l'authentification – assurer l'identification et l'authentification de toutes les personnes dûment autorisées, en fonction de leurs compétences, avant toute opération;

- autorisation – autoriser les participants à avoir accès aux données du Registre électoral, en fonction de leurs compétences.[14]

L'Autorité électorale permanente est autorisée à prendre des mesures de prévention des pertes d'information et d'assurance de leur récupération suite à des événements fortuite ou en cas de force majeure.

Le Centre National de Réponse aux Cyber Incidents – CERT-RO fait des audits de sécurité du Registre électoral.

La responsabilité d'assurer la protection et la confidentialité des données personnelles dans le Registre électoral appartient, selon la loi, à l'Autorité électorale permanente et au personnel autorisé des mairies.

§.3. La vérification de l'éligibilité des électeurs

[14] Ibidem.

En Roumanie, jusqu'en 2016, dans le jour de vote on a utilisé seulement des méthodes traditionnelles, le timbre, l'encre et le papier étant la technologie standard dans cette procédure. Une situation particulière a existé lors du référendum national sur la révision de la Constitution en 2003, lorsqu'un système de vote électronique utilisant des ordinateurs dans les bureaux de vote avait été mis en place pour les militaires dans les théâtres d'opérations. Sur chaque ordinateur du bureau de vote, l'on avait installé pour communiquer avec le système de vote électronique, un certificat numérique émis à cet égard, ainsi que le programme informatique nécessaire pour la connexion à Internet. En outre, la communication entre le système de vote électronique et les ordinateurs dans les isoloirs avait été faite exclusivement sur la base des certificats numériques émis par le système dans le seul but d'assurer la sécurité et l'intégrité de cette communication.

Bien qu'utilisé une fois et par un très petit nombre d'électeurs, le vote électronique a également influencé la loi pénale, l'impression et l'utilisation de fausses données d'accès, l'accès frauduleux du système de vote électronique ou la contrefaçon par tous les moyens des bulletins de vote électroniques ayant considéré une infraction pénale passible d'une peine d'emprisonnement de 1 à 5 ans.

À partir de 2016, l'Autorité électorale permanente et le Service spécial des télécommunications ont mis en place un système informatique de surveillance du taux de participation et de prévention du vote illégal qui vise à:

a) vérifier si les électeurs remplisse les conditions d'exercer le droit de vote;

b) identifier toute tentative de vote multiple ou de vote sans en avoir le droit;

d) assurer le suivi en temps réel de la participation électorale.

En substance, la procédure de vote implique que chaque électeur présente sa carte d'identité à l'opérateur informatique du bureau de vote, qui introduit le code d'identification personnel dans le système informatique pour vérifier la conformité et empêcher le vote illégal. Cet enregistrement est effectué sur les tablettes fournies par le Service spécial de télécommunications, par la récupération automatique du code d'identification personnel en photographiant l'identifiant ou en introduisant manuellement le code d'identification personnel.

En enregistrant les codes d'identification personnels des électeurs dans le Système informatique de surveillance de la participation électorale et de prévention du vote illégal, le bureau électoral a la possibilité de contrôler en temps réel, si l'électeur est affecté au bureau de vote, s'il remplit les conditions d'exercer les droits de vote (par exemple: il a plus de 18 ans ou il / elle n'a jamais été condamné) et si l'électeur n'a pas déjà voté dans un autre bureau de vote ou par correspondance.

Une fois les bureaux de vote fermés, le module de vérification est désactivé, au lieu d'activer un module de collecte pour les résultats du vote. Les opérateurs informatiques saisissent les données dans le formulaire électronique consacré à cet but, ce qui indique des contradictions basées sur des clés de vérification, puis les transmet au serveur principal du Bureau électoral central.

Pour l'Autorité électorale permanente et le Service spécial des télécommunications, il est devenu évident que la mise en œuvre d'un système d'information aussi complexe comportait de multiples risques et menaces cybernétiques.

Pour cette raison, l'équipement de protection contre les incidents de cybersécurité a été intégré dans le Système d'information central et la responsabilité de la sécurité de l'ensemble du système a été confiée au Service spécial des télécommunications, institution publique chargée d'assurer la sécurité nationale en cybernétique des affaires, avec le pouvoir de donner des instructions de sécurité similaires à celles de l'Autorité électorale permanente pour le Registre électoral.

§.4. La centralisation des résultats et la répartition des sièges

Tout de même en Roumanie la centralisation des résultats es sujet sensible pour le public de point de vue de la tradition des fraudes électorales datant depuis 1857, mais aussi à cause de la façon dont la fameuse citation «peu importe qui vote, mais qui compte les votes» " résonne dans l'imaginaire politique roumain.

C'est probablement la raison pour laquelle la première intersection entre la technologie de l'information avec les processus électoraux en Roumanie a concerné la centralisation et la répartition des sièges.

Si au début, les données des transcriptions étaient introduites dans des ordinateurs par des opérateurs humains, les élections locales en 2004 avaient déjà été effectuées en scannant les transcriptions des résultats de vote dans les bureaux électoraux de circonscription, en les numérisant et en les envoyant à distribution et attribution des sièges au serveur principal du Bureau central des élections.

Le rôle de garant de la sécurité informatique dans ce domaine est partagé entre l'Autorité électorale permanente et le Service spécial des télécommunications. L'Autorité électorale permanente définit les exigences de sécurité des applications et des services informatiques requis par le Bureau électoral central pour centraliser les résultats de vote, et les communications de données et de voix nécessaires pour centraliser les résultats des élections et, implicitement, leur sécurité est fournie par le Service Spécial des Télécommunications.

L'importance de la sécurité du système d'information pour la centralisation des résultats est attestée par la protection prévue par la loi pénale. Ainsi, la mise en service ou l'utilisation d'un programme informatique avec des vices qui altère l'enregistrement ou la centralisation des résultats obtenus dans les bureaux de vote ou détermine la répartition des sièges en dehors des dispositions légales, sera punie d'un emprisonnement de 2 à 7 ans et l'interdiction d'exercer certains droits. La même sanction s'applique pour l'introduction de données, d'informations ou de procédures qui modifient le système d'information national nécessaire à l’établissement des résultats des élections.

§.5. Conclusion

J'apprécie que cette brève présentation ait réussi à accentuer l'importance offerte par la législature roumaine à la technologie de l'information et à sa sécurité. Bien sûr, celles mentionnées ne peuvent pas couvrir toutes les mesures de sécurité proactives et réactives que l'Autorité électorale permanente et les autres institutions impliquées dans les élections prennent pour protéger l’espace cybernétique électoral, celles-ci continuant à évoluer et à passer d'un processus électoral à l'autre.

D'un autre côté, je voudrais mentionner que le concept de cybersécurité maintient des tensions importantes avec le principe de la nature publique des élections,

car la capacité de l'électeur ordinaire à comprendre comment la sécurité des technologies dans le processus électoral est assurée, n'est jamais assez élevée pour lui permettre de l'évaluer correctement.

Pour la même raison, les risques et les cybermenaces sont toujours des prétextes pour justifier les réticences qui entourent l'introduction de nouvelles technologies dans les élections, comme le vote électronique ou les urnes de vote électroniques. Par exemple, toutes les initiatives concernant le vote électronique sen Roumanie, en tant que méthode alternative à la traditionnelle, ont été rejetées parce qu'elles étaient incapables d'expliquer comment assurer la sécurité et, par conséquent, comment renforcer la confiance des électeurs sur l'intégrité du système de vote électronique.

Bibliographie:

1. La stratégie de cyber-sécurité de la Roumanie ;

2. La Stratégie de cybersécurité de l'Union européenne: un cyberespace ouvert, sûr et sécurisé ;

3. Loi n° 208/2015 concernant l'élection du Sénat et de la Chambre des Députés, ainsi que portant sur l'organisation et le fonctionnement de l'Autorité électorale permanente.

4. Le développement des concepts de sécurité - https://studiidesecuritate.wordpress.com/2011/08/11/evolutia-conceptelor-de-securitate/