MINISTÈRE
DE L'EUROPE
ET DES AFFAIRES
ÉTRANGÈRES

Liberté
Égalité
Fraternité

DIRECTION DES RESSOURCES HUMAINES

SOUS-DIRECTION DE L'ATTRACTIVITÉ ET DES RECRUTEMENTS

Bureau des concours et examens professionnels

Concours interne et externe de secrétaire des systèmes d'information et de communication au titre de l'année 2024

Épreuves écrites d'admissibilité

Du 27 au 28 février 2024

Note de synthèse

Durée totale de l'épreuve : 3 heures – coefficient 2

Toute note inférieure à 6 sur 20 est éliminatoire

Note de synthèse, établie à partir d'un dossier à caractère scientifique et technique de vingt-cinq pages maximum permettant de vérifier les qualités d'expression, d'analyse et de synthèse du candidat dans les domaines scientifiques et techniques, ainsi que son aptitude à dégager des conclusions et à formuler des propositions

Ce dossier comporte 25 pages (page de garde, sujet et sommaire non compris)

SUJET

« Comme le changement climatique, la transformation numérique fait partie des phénomènes qui définissent notre époque : ils sont intimement liés à nos modes de vie et constituent dans le même temps des enjeux déterminants du nouvel ordre mondial. » Jean-Yves Le Drian, ministre de l'Europe et des Affaires étrangères.

Le 29 juin 2021, le ministère de l'Europe et des Affaires étrangères (MEAE) s'est engagé dans un plan de transformation numérique pour faciliter au quotidien les procédures pour les Français et Françaises de l'étranger, pour l'ensemble des usagers ainsi que pour soutenir les missions du ministère. La démarche s'inscrit dans une approche écoresponsable et cherche à améliorer à la fois le service rendu et la qualité de vie au travail des agentes et agents.

Vous venez de prendre vos fonctions de secrétaire des systèmes d'information et de communication dans votre nouveau poste à l'étranger. En vue des prochaines élections, l'Ambassadeur vous demande de lui faire un point sur l'environnement de la transformation numérique au MEAE et sur le vote par internet.

Avertissement : La note doit pouvoir être intelligible pour une personne non spécialiste du domaine numérique et se limiter aux éléments du dossier. Vous veillerez également à structurer au mieux votre copie. Enfin, toute recopie, même partielle, des textes du dossier sera sanctionnée.

SOMMAIRE

Texte 1

E-administration : du PAGSI au programme Action publique 2022

Dernière modification : 4 octobre 2021

Par : La Rédaction

La transformation numérique de l'État est continue depuis plus de 20 ans. Grâce à l'évolution des technologies, de nombreux services dématérialisés ont été créés (téléservices, simulateurs, etc.). Aujourd'hui, le numérique est devenu le premier canal d'accès aux services publics.

Le programme Action publique 2022, lancé par le gouvernement fin 2017, constitue une nouvelle étape de la transformation numérique des administrations. Les 250 démarches les plus courantes doivent être dématérialisées d'ici mai 2022. Une administration plus proactive (échanges de données entre administrations, information des citoyens ...), l'ouverture des données publiques et les projets d'intelligence artificielle sont encouragés afin d'offrir de nouveaux services.

Une e-administration en constant déploiement depuis 20 ans

La période 1998-2007

Depuis 1998, les pouvoirs publics ont élaboré plusieurs programmes ou plans en vue de développer l'administration électronique. Ce mouvement débute avec le **programme d'action gouvernemental pour la société de l'information (PAGSI)**. Il débouche notamment sur l'adoption par les ministères de programmes pluriannuels de modernisation (PPM) et sur la création en 2000 du portail de l'administration, Service-public.fr.

La politique poursuivie vise à faire de l'État un acteur exemplaire et un accélérateur, plus transparent et plus efficace, en facilitant la diffusion en ligne des informations publiques essentielles et en généralisant les téléprocédures. Il s'agit de mettre en place "une administration à accès pluriel" pour les usagers (guichets physiques, courriers, services en ligne ou téléphonie).

Ce mouvement de modernisation se poursuit avec le **plan ADministration ÉLEctronique (ADELE)** sur la période 2004-2007. La finalité de ce plan, doté d'un budget de 1,8 milliard d'euros, est de faire de l'administration électronique un levier de la modernisation de l'État. Le plan prévoit 140 mesures afin que l'ensemble des démarches administratives puissent être accomplies à distance par téléphone ou par internet à l'horizon 2006. L'agence pour le

développement de l'administration électronique (ADAE), créée en 2003 auprès du Premier ministre, assure la mise en œuvre du plan.

La période 2008-2018

En 2008, le **plan "France numérique 2012"** prend le relais d'ADELE. Il a notamment pour but d'accroître l'accessibilité des sites Internet publics, de développer le paiement en ligne, d'améliorer l'interopérabilité entre administrations et d'ouvrir les données publiques (*open data*). Selon un bilan présenté en novembre 2011 par le gouvernement, le plan "France numérique 2012" a permis la dématérialisation de 76% des procédures les plus attendues par les usagers. Un référentiel général d'interopérabilité (RGI) est publié en 2009 et valorise les standards ouverts. Quant à la politique d'ouverture des données, elle se concrétise par la création fin 2011 de la plateforme de données publiques, data.gouv.fr, développée par la mission Etalab. Cette structure, placée sous l'autorité du Premier ministre, est également née en 2011.

En 2012, le **Secrétariat général à la modernisation de l'action publique (SGMAP)** est institué. Il est chargé de mettre en œuvre la politique de modernisation de l'État, notamment en matière numérique. Des comités interministériels de la modernisation de l'action publique (CIMAP) décident des actions à engager, conformément au "choc de simplification" annoncé par le président de la République en mars 2013.

Une nouvelle stratégie technologique de l'État est mise en place *via* le réseau interministériel de l'État (RIE) et le projet dit de **"l'État plateforme"**. Un décret du 1er août 2014 place les différents systèmes d'information (SI) ministériels sous la gouvernance du Premier ministre en créant un système d'information unifié de l'État (socle matériel et logiciel commun).

La même année, le gouvernement présente un projet pour faire du numérique l'instrument de la transformation de l'État. 40 nouvelles mesures de simplification des démarches administratives pour les particuliers sont annoncées. La majorité correspond à la création par les ministères de nouveaux services numériques (par exemple simulateur pour estimer ses droits aux prestations sociales). Un administrateur général des données est nommé pour animer et impulser la politique d'*open data* au sein des administrations de l'État.

Fin 2015, les usagers se voient proposer un nouveau service numérique : celui de saisir par voie électronique (SVE) - dans les mêmes conditions qu'une saisine postale - les administrations d'État pour près de neuf démarches administratives sur dix. Cette saisine peut être effectuée par le biais d'une téléprocédure, d'un formulaire de contact ou par courriel.

En 2016, France Connect est déployé. Cet outil permet d'utiliser un compte, un identifiant et un mot de passe uniques pour tous les services publics en ligne (impôts, caisse d'allocations familiales, mairie, etc.). La refonte du site Service-public.fr a également lieu. 2016 est aussi marquée par la publication de la loi pour une République numérique, dite loi "Lemaire". Elle impose notamment aux administrations d'ouvrir leurs données publiques par défaut, y compris leurs algorithmes, de plus en plus fréquents dans les décisions administratives (par exemple pour le calcul de l'impôt). La loi crée, en outre, un service public de la donnée.

En 2017, le **plan "Préfectures nouvelle génération" (PPNG)** est mis en œuvre. Les procédures de délivrance des titres (demande de permis de conduire ou de carte grise, pré-demande de passeport ou carte d'identité) sont dématérialisées. La réforme repose sur

l'Agence nationale des titres sécurisés (ANTS) et les nouveaux centres d'expertise et de ressources des titres (CERT) répartis sur tout le territoire. La mise en place de la téléprocédure pour obtenir sa carte grise a cependant rencontré de nombreuses difficultés qui ont provoqué d'importants retards dans la délivrance des titres.

Pour concevoir des services publics innovants dans des délais courts, des **"startups d'État"** au sein du SGMAP se multiplient, des "entrepreneurs d'intérêt général" (EIG) sont recrutés pour dix mois dans les administrations. Des hackathons sur deux jours regroupant des développeurs, chefs de projets, etc., des administrations de l'État sont aussi organisés.

D'après l'indice relatif à l'économie et à la société numériques (DESI, pour *Digital Economy and Society Index*) publié par la Commission européenne en mai 2018, la France était à la 13e place européenne en matière de services publics numériques. Elle disposait d'une note moyenne en ce qui concerne l'étendue des services en ligne (87 contre 84 pour la moyenne européenne). En revanche, elle était en avance en matière de données ouvertes (4e place en Europe).

La transformation numérique de l'État dans le cadre d'Action publique 2022

Le programme Action publique 2022, programme de réforme de l'État lancé par le gouvernement en octobre 2017, reprend pour priorité la transformation numérique des administrations. Ce programme est piloté par la direction interministérielle du numérique (DINUM), service du Premier ministre, et par la direction interministérielle de la transformation publique (DITP), rattachée au ministère de la transformation et de la fonction publiques.

Améliorer la qualité des services publics par l'innovation numérique

La transformation numérique est l'un des cinq chantiers transverses d'Action publique 2022. Six comités interministériels de la transformation publique (CITP), qui se sont tenus depuis février 2018, en ont détaillé le programme. Le gouvernement entend tirer parti de la révolution numérique (intelligence artificielle - IA-, *open data*, etc.) pour offrir des services innovants, tout en réduisant les coûts.

Parmi les diverses réformes mises en oeuvre figurent :

- de nouveaux services en ligne (création d'un code du travail numérique ...)
- un guichet unique internet des formalités pour les entreprises, confié à l'Institut national de la propriété intellectuelle (INPI) ;
- "France Expérimentation", un dispositif facilitant la mise en œuvre du droit à l'expérimentation pour les entreprises porteuses de projets innovants ;
- le mise en place d'un bouton "je donne mon avis" à la fin des démarches administratives en ligne ;
- un observatoire de la qualité des démarches en ligne créé en juin 2019, qui permet de suivre l'avancée et la qualité de la dématérialisation, selon huit critères de qualité ;
- le lancement en janvier 2021 du programme Services publics + pour améliorer l'efficacité des services publics en continu ;
- des plans de transformation numérique dans chaque ministère ;

- un laboratoire pour l'intelligence artificielle (Lab IA) interministériel pour accompagner les administrations dans le déploiement de leurs projets d'IA et anticiper les effets de l'IA sur les métiers et la relation aux usagers.

D'autres mesures sont encore annoncées comme :

- la simplification d'ici janvier 2022 de dix démarches emblématiques (dématérialisation de la demande de permis de construire...) et des 100 formulaires les plus utilisés par les usagers ;
- la dématérialisation d'ici mai 2022 des 250 démarches administratives les plus utilisées par les Français. L'objectif initial fixé par le gouvernement en 2017 de 100% des démarches dématérialisées à l'horizon 2022 a été recentré en 2019 sur ces 250 démarches ;
- un partage des données des usagers entre administrations par défaut (selon le principe "dites-le-nous une fois ") ;
- l'accélération du chantier FranceConnect avec pour objectif 30 millions d'utilisateurs fin 2022 (contre 500 000 début 2017 et 20 millions en 2021) ;
- la simplification de la demande de subvention des associations, en allant vers le modèle d'un guichet unique ;
- l'accélération de la numérisation des processus internes à l'administration, avec l'objectif d'une administration "zéro papier" afin de simplifier et fluidifier le travail et les circuits de décision ;
- une administration proactive et plus proche, qui anticipe les besoins des usagers afin de lutter contre les non-recours et simplifier l'accès aux démarches ;
- une politique des données publiques plus ambitieuse. La politique de la donnée devient une priorité stratégique de l'État (circulaire du Premier ministre du 27 avril 2021 qui fait suite au rapport Bothorel remis en décembre 2020). Chaque ministère doit élaborer une feuille de route et désigner un administrateur des données, des algorithmes et des codes sources. Un plan d'actions dédié à l'animation et à la promotion interministérielle du logiciel libre et des *communs* va être lancé. 15 feuilles de route ministérielles des données, algorithmes et codes sources ont été rendues publiques le 27 septembre 2021 ;
- une nouvelle stratégie *Cloud* de l'État afin notamment que les données des usagers soient sécurisées et protégées ;
- un chantier de prospective sur le futur du numérique public à l'horizon 2030.

Les mesures d'accompagnement des agents prévues

Pour mettre en œuvre la transformation des services publics, le gouvernement a prévu d'accompagner les agents publics.

De nombreux outils sont proposés par la DITP. Ainsi, démarches-simplifiées.fr, offre aux administrations et agents qui ont besoin de dématérialiser des démarches des usagers un générateur de formulaires et une plateforme d'instruction de dossiers.

Un futur "sac à dos numérique de l'agent public" est en cours de conception. Il doit permettre aux agents de l'État de travailler à distance plus facilement et de façon plus sécurisée (visioconférence, messagerie instantanée...). La crise du Covid-19 a déjà fortement accéléré le télétravail. Pour assurer la continuité de l'administration numérique, l'État a dû équiper rapidement ses agents. Au 1er mars 2020, avant le premier confinement, seulement 22%

d'entre eux disposait d'un ordinateur portable. Au 1er juillet 2021, ce pourcentage atteint 85%. Fin 2021, tous les personnels dont les fonctions sont télétravaillables devraient être équipés.

L'État souhaite également attirer les talents du numérique. Plusieurs plans ont été lancés. Le dernier date de mai 2021. Il vise à renforcer l'attractivité, la formation et les parcours de carrière dans la filière du numérique publique.

Les investissements dédiés

Outre les outils, des moyens financiers accompagnent la transformation des administrations.

Un fonds pour la transformation de l'action publique, au titre du Grand plan d'investissement 2018-2022, a ainsi été créé. Il est doté de 700 millions d'euros sur cinq ans pour accompagner les administrations centrales et déconcentrées dans leurs projets de transformation et de simplification.

Plus récemment, dans le cadre du **plan de relance,** une enveloppe d'un milliard d'euros est consacrée à la transformation numérique de l'État. Dans le plan, un **fonds d'innovation et de transformation numérique (FITN)** est doté de 292 millions d'euros. Un guichet unique permettant aux administrations de déposer leurs projets a été mis en place.

Commission nationale de l'informatique et des libertés

Délibération n° 2019-053 du 25 avril 2019 portant adoption d'une recommandation relative à la sécurité des systèmes de vote par correspondance électronique, notamment via Internet

NOR : *CNIL1917529X*

La Commission nationale de l'informatique et des libertés,

Vu la convention n° 108 du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel ;

Vu le règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE ;

Vu le code électoral ;

Vu la loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés, notamment son article 11-I-2°-a *bis)* ;

Vu le décret n° 2005-1309 du 20 octobre 2005 modifié pris pour l'application de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés ;

Après avoir entendu Mme Dominique CASTERA, commissaire, en son rapport, et Mme Nacima BELKACEM, commissaire du Gouvernement, en ses observations ;

Formule les observations suivantes :

A titre liminaire, la commission observe que le constat, réalisé lors de l'adoption de sa recommandation de 2010, du développement et de l'extension des systèmes de vote par correspondance électronique, notamment *via* Internet, à un nombre croissant d'opérations de vote et de types de vote, reste d'actualité.

La commission souligne que le recours à de tels systèmes doit s'inscrire dans le respect des principes fondamentaux qui commandent les opérations électorales : le secret du scrutin sauf pour les scrutins publics, le caractère personnel et libre du vote, la sincérité des opérations électorales, la surveillance effective du vote et le contrôle *a posteriori* par le juge de l'élection. Ces systèmes de vote par correspondance électronique, notamment *via* Internet, doivent également respecter les prescriptions des textes constitutionnels, législatifs et réglementaires en vigueur.

Devant l'extension continue du vote par Internet à tous types d'élections, la commission souhaite rappeler que le vote par correspondance électronique, notamment *via* Internet, présente des difficultés accrues au regard des principes susmentionnés pour les personnes chargées d'organiser le scrutin et celles chargées d'en vérifier le déroulement, principalement à cause de l'opacité et de la technicité importante des solutions mises en œuvre, ainsi que de la très grande difficulté de s'assurer de l'identité et de la liberté de choix de la personne effectuant les opérations de vote à distance.

Au cours des travaux que la commission a menés depuis 2003 et compte tenu des menaces qui pèsent sur ces dispositifs, elle a, en effet, pu constater que les systèmes de vote existants ne fournissaient pas encore toutes les garanties exigées par les textes légaux. Dès lors et en particulier, compte-tenu des éléments précités, la commission reste réservée quant à l'utilisation de dispositifs de vote par correspondance électronique, notamment *via* Internet, pour des élections politiques.

La présente délibération a pour objet de revoir la recommandation de 2010 à l'aune des opérations électorales intervenues depuis, de l'évolution des solutions de vote proposées par les prestataires du secteur, des retours effectués par les différentes parties prenantes, des contrôles réalisés par la CNIL ainsi que de l'évolution du cadre juridique relatif à la protection des données.

La nouvelle recommandation a pour champ d'application les dispositifs de vote par correspondance électronique, en particulier *via* Internet. Elle ne concerne pas les dispositifs de vote par codes-barres, les dispositifs de vote par téléphone fixe ou mobile, ni les systèmes informatiques mis à disposition des votants sous forme de boîtiers de vote ou en isoloirs (dites « machines à voter »). Elle est destinée à fixer, de façon pragmatique, les objectifs de sécurité que doit atteindre tout dispositif de vote par correspondance électronique, notamment *via* Internet, en fonction des risques que présente le déroulement du vote. Les réponses apportées par les systèmes à ces objectifs de sécurité doivent ainsi prendre en compte le contexte et les menaces qui pèsent sur le scrutin.

Elle vise également à s'appliquer aux futures évolutions des systèmes de vote par correspondance électronique, notamment *via* Internet, en vue d'un meilleur respect des principes de protection des données personnelles, et à éclairer les responsables de traitement sur le choix des dispositifs de vote par correspondance électronique à retenir.

Elle abroge la délibération n° 2010-371 du 21 octobre 2010 portant adoption d'une recommandation relative à la sécurité des systèmes de vote électronique.

Compte tenu de ces observations préalables, la commission émet la recommandation suivante.

Le niveau de risque du scrutin

Le niveau de risque que présente le déroulement d'un vote varie en fonction du type de scrutin, des évènements redoutés et des menaces qui pèsent sur le traitement. Ainsi, la commission recommande que la solution utilisée pour le scrutin tienne compte de l'importance du niveau de risque de l'élection ainsi que des éventuels bénéfices pour les parties prenantes de recourir à un système de vote par correspondance électronique et que la solution choisie réponde à tous les objectifs de sécurité fixés au regard de ce niveau de risque.

La commission identifie trois niveaux de risque :

– **Niveau 1 :** Les sources de menace, parmi les votants, les organisateurs du scrutin ou les personnes extérieures, ont peu de ressources et peu de motivations. L'administrateur (ou les administrateurs) du système d'information n'est ni électeur, ni candidat. Il est considéré comme neutre par toutes les parties. Ce niveau s'applique pour les scrutins impliquant peu d'électeurs, se déroulant dans un cadre non conflictuel, à l'issue duquel les personnes élues auront peu de pouvoirs, comme par exemple l'élection d'un représentant de classe. Le scrutin ne présente pas de risques importants.
– **Niveau 2 :** Les sources de menace, parmi les votants, les organisateurs du scrutin, les personnes extérieures, au sein du prestataire ou du personnel interne, peuvent présenter des ressources moyennes ou des motivations moyennes. Ce niveau s'applique à des scrutins impliquant un nombre important d'électeurs et présentant un enjeu élevé pour les personnes mais dans un contexte dépourvu de conflictualité particulière. Il s'agit par exemple des élections de représentants du personnel au sein d'organismes ou encore au sein d'un ordre professionnel. Le scrutin présente un risque modéré.
– **Niveau 3 :** Les sources de menace, parmi les votants, les organisateurs du scrutin, les personnes extérieures, au sein du prestataire ou du personnel interne, peuvent présenter des ressources importantes ou de fortes motivations. Ce niveau concerne les scrutins impliquant un nombre important d'électeurs et présentant un enjeu très élevé, dans un climat potentiellement conflictuel. Il s'agit par exemple d'élections de représentants du personnel au sein d'organisations importantes, à grande échelle et dans un cadre conflictuel. Le scrutin présente un risque important.

La commission déconseille d'utiliser un dispositif de vote par correspondance électronique, notamment *via* Internet, dans l'hypothèse où les sources de menace peuvent disposer à la fois de ressources importantes et d'une motivation forte.

Le responsable du traitement identifie le niveau correspondant à sa situation en fonction des risques soulevés par son scrutin. A cette fin la commission propose, de manière facultative et à titre d'exemple, une grille d'analyse simplifiée, basée sur des questions fermées, ayant pour objet de guider et d'aider les responsables de traitement le désirant à se positionner sur cette échelle. Cette grille d'analyse est placée au sein de la fiche pratique.

En cas de doute entre deux niveaux, le niveau le plus élevé devrait être privilégié. Le responsable de traitement, maitrisant le périmètre, les enjeux et le contexte de son scrutin, est libre de choisir le niveau de risque qu'il juge approprié, dès lors qu'il peut justifier son analyse auprès de la commission et de l'expert indépendant.

Une fois son niveau de risque identifié, le responsable de traitement peut déterminer les objectifs de sécurité que la solution de vote doit atteindre.

Le choix du niveau de risque par le responsable de traitement étant évalué par l'expert indépendant mandaté (voir ci-après) pour garantir la conformité des opérations de vote à la présente recommandation, il convient que le responsable de traitement lui fournisse les éléments ayant été pris en compte dans la détermination de ce niveau.

D'une manière générale, la commission rappelle que les traitements de données personnelles, dont les dispositifs de vote, qui remplissent au moins deux des critères suivants doivent en principe faire l'objet d'une analyse d'impact relative à la protection des données (AIPD) :

– évaluation/« *scoring* » (y compris le profilage) ;
– décision automatique avec effet légal ou similaire ;
– surveillance systématique ;
– collecte de données sensibles (opinions politiques et appartenances syndicales notamment) ;
– collecte de données personnelles à large échelle ;
– croisement de données ;
– personnes vulnérables (patients, personnes âgées, enfants, etc.) ;
– usage innovant (utilisation d'une technologie nouvelle) ;
– exclusion du bénéfice d'un droit/contrat.

Dès lors, au regard des critères relatifs aux données sensibles et à la collecte de données à large échelle et compte tenu du contexte du scrutin le cas échéant, il peut être nécessaire que le responsable de traitement réalise une AIPD.

Les objectifs de sécurité à atteindre en fonction du niveau de risque

Chaque niveau de risque se voit associer des objectifs de sécurité qui permettent de définir le niveau de sécurité attendu. Ces objectifs sont cumulables, le niveau 2 étant composé d'objectifs de sécurité spécifiques et des objectifs de sécurité du niveau 1, le niveau 3 étant, quant à lui, composé d'objectifs de sécurité spécifiques et des objectifs de sécurité des deux niveaux précédents.

La commission proposera sur son site web ou tout autre support utile, une fiche pratique présentant des exemples permettant d'atteindre les objectifs de sécurité précités. Les industriels peuvent, s'ils le souhaitent, proposer à la

commission des exemples de moyens permettant d'atteindre les objectifs afin que cette fiche puisse être agrémentée de ces informations. La commission sera seule juge de la pertinence des moyens proposés.

Cette fiche détaillera ce qui est attendu derrière chaque objectif de sécurité.

Les solutions de vote dont le scrutin présente un risque de niveau 1 doivent atteindre *a minima* l'ensemble des objectifs de sécurité suivants :

– Objectif de sécurité n° 1-01 : Mettre en œuvre une solution technique et organisationnelle de qualité ne présentant pas de faille majeure (faille publiée par l'éditeur et/ou rendue publique par des tiers).
– Objectif de sécurité n° 1-02 : Définir le vote d'un électeur comme une opération atomique, c'est-à-dire comme comportant de manière indivisible le choix, la validation, l'enregistrement du bulletin dans l'urne, l'émargement et la délivrance d'un récépissé.
– Objectif de sécurité n° 1-03 : Authentifier les électeurs en s'assurant que les risques majeurs liés à une usurpation d'identité sont réduit de manière significative.
– Objectif de sécurité n° 1-04 : Assurer la stricte confidentialité du bulletin dès sa création sur le poste du votant.
– Objectif de sécurité n° 1-05 : Assurer la stricte confidentialité et l'intégrité du bulletin pendant son transport.
– Objectif de sécurité n° 1-06 : Assurer, de manière organisationnelle et/ou technique, la stricte confidentialité et l'intégrité du bulletin pendant son traitement et son stockage dans l'urne jusqu'au dépouillement.
– Objectif de sécurité n° 1-07 : Assurer l'étanchéité totale entre l'identité de votant et l'expression de son vote pendant toute la durée du traitement.
– Objectif de sécurité n° 1-08 : Renforcer la confidentialité et l'intégrité des données en répartissant le secret permettant le dépouillement exclusivement au sein du bureau électoral et garantir la possibilité de dépouillement à partir d'un seuil de secret déterminé.
– Objectif de sécurité n° 1-09 : Définir le dépouillement comme une fonction atomique utilisable seulement après la fermeture du scrutin.
– Objectif de sécurité n° 1-10 : Assurer l'intégrité du système, de l'urne et de la liste d'émargement.
– Objectif de sécurité n° 1-11 : S'assurer que le dépouillement de l'urne puisse être vérifié a posteriori.

Les solutions de vote dont le scrutin présente un risque de niveau 2 doivent atteindre *a minima* l'ensemble des objectifs de sécurité du niveau 1 ainsi que les suivants :

– Objectif de sécurité n° 2-01 : Assurer une haute disponibilité de la solution.
– Objectif de sécurité n° 2-02 : Assurer un contrôle automatique de l'intégrité du système, de l'urne et de la liste d'émargement.
– Objectif de sécurité n° 2-03 : Permettre le contrôle automatique par le bureau électoral de l'intégrité de la plateforme de vote pendant tout le scrutin.
– Objectif de sécurité n° 2-04 : Authentifier les électeurs en s'assurant que les risques majeurs et mineurs liés à une usurpation d'identité sont réduits de manière significative.
– Objectif de sécurité n° 2-05 : Assurer un cloisonnement logique entre chaque prestation de vote de sorte qu'il soit possible de stopper totalement un scrutin sans que cela ait le moindre impact sur les autres scrutins en cours.
– Objectif de sécurité n° 2-06 : Utiliser un système d'information mettant en œuvre les mesures de sécurité physique et logique recommandées par les éditeurs et l'ANSSI.
– Objectif de sécurité n° 2-07 : Assurer la transparence de l'urne pour tous les électeurs.

Les solutions de vote dont le scrutin présente un risque de niveau 3 doivent atteindre *a minima* l'ensemble des objectifs de sécurité des niveaux 1 et 2, ainsi que les suivants :

– Objectif de sécurité n° 3-01 : Etudier les risques selon une méthode éprouvée afin de définir les mesures les plus adéquates au contexte de mise en œuvre.
– Objectif de sécurité n° 3-02 : Permettre la transparence de l'urne pour tous les électeurs à partir d'outils tiers.
– Objectif de sécurité n° 3-03 : Assurer une très haute disponibilité de la solution de vote en prenant en compte les risques d'avarie majeure.
– Objectif de sécurité n° 3-04 : Permettre le contrôle automatique et manuel par le bureau électoral de l'intégrité de la plateforme pendant tout le scrutin.
– Objectif de sécurité n° 3-05 : Assurer un cloisonnement physique entre chaque prestation de vote de sorte qu'il soit possible de stopper totalement un scrutin sans que cela ait le moindre impact sur les autres scrutins en cours.

Le responsable de traitement ou son prestataire sont libres d'utiliser toute solution leur permettant d'atteindre les objectifs de sécurité énoncés.

Quel que soit le niveau déterminé, il convient de fournir aux électeurs, en temps utile, une note explicative détaillant clairement les opérations de vote ainsi que le fonctionnement général du système de vote par correspondance électronique, notamment *via* Internet. Cette notice explicative ne se substitue pas à l'obligation d'information imposée par les articles 13 et 14 du règlement européen sur la protection des données (RGPD) s'agissant du traitement des données.

Parallèlement, la commission tient à souligner que, de par leur nature et sensibilité, les plateformes de vote par correspondance électronique, notamment via Internet, se doivent d'être accessibles à toutes personnes, notamment

aux personnes en situation de handicap et en particulier visuel. Ainsi, pour les organismes du secteur public ou délégataires d'une mission de service public désirant proposer ce service à ses électeurs, il est nécessaire que le système de vote respecte le référentiel général d'accessibilité pour les administrations (RGAA). Pour les organismes non soumis à ce référentiel, il est fortement recommandé d'en suivre les prescriptions afin de mettre l'ensemble des votants en capacité d'exprimer leur suffrage par ce moyen.

L'expertise du système de vote par correspondance électronique, notamment *via* Internet

Tout responsable de traitement mettant en œuvre un système de vote par correspondance électronique, notamment *via* Internet, doit faire expertiser sa solution par un expert indépendant, que la solution de vote soit gérée en interne ou fournie par un prestataire.

L'expertise doit couvrir l'intégralité du dispositif installé avant le scrutin (logiciel, serveur, etc.), la constitution des listes d'électeurs et leur enrôlement et l'utilisation du système de vote durant le scrutin et les étapes postérieures au vote (dépouillement, archivage, etc.).

L'expertise doit porter sur l'ensemble des éléments décrits dans la présente délibération et notamment sur :

– le code source correspondant à la version du logiciel effectivement mise en œuvre ;
– les mécanismes de scellement utilisés aux différentes étapes du scrutin ;
– le système informatique sur lequel le vote va se dérouler ;
– les échanges réseau ;
– les mécanismes de chiffrement utilisés, notamment pour le chiffrement du bulletin de vote ;
– les mécanismes d'authentification des électeurs et la transmission des secrets à ces derniers ;
– l'évaluation du niveau de risque du scrutin ;
– la pertinence et l'effectivité des solutions apportées par la solution de vote aux objectifs de sécurité.

L'expertise doit porter sur l'ensemble des éléments constituant la solution de vote.

Lors de scrutins présentant un niveau de risque 2 ou 3, l'expert réalise des audits sur la plateforme, afin de s'assurer de la cohérence et de l'effectivité des solutions apportées, par le biais de tests d'intrusions notamment. L'ensemble des opérations effectuées dans ce cadre est annexé au rapport d'expertise.

L'expertise doit être réalisée par un expert indépendant, c'est-à-dire qu'il devra répondre aux critères suivants :

– être un informaticien spécialisé dans la sécurité ;
– ne pas avoir d'intérêt dans la société qui a créé la solution de vote à expertiser, ni dans l'organisme responsable de traitement qui a décidé d'utiliser la solution de vote ;
– posséder si possible une expérience dans l'analyse des systèmes de vote, en ayant expertisé les systèmes de vote par correspondance électronique, notamment *via* Internet, d'au moins deux prestataires différents.

Le rapport d'expertise, et ses annexes doivent être remis au responsable de traitement et aux prestataires de solution de vote par correspondance électronique, notamment *via* Internet.

Si l'expertise peut couvrir un champ plus large que celui de la présente recommandation, le rapport d'expertise fourni au responsable de traitement doit comporter une partie spécifique présentant l'évaluation du dispositif au regard des différents points de la recommandation.

L'expert doit fournir un moyen technique permettant de vérifier *a posteriori* que les différents composants logiciels sur lesquels a porté l'expertise n'ont pas été modifiés sur le système utilisé durant le scrutin. La méthode et les moyens permettant d'effectuer cette vérification doivent être décrits dans le rapport d'expertise. Pour ce faire, l'expert peut, par exemple, utiliser des empreintes numériques.

L'expertise portant sur une solution mise en œuvre pour un scrutin dont le niveau de risque est évalué à 1 peut reprendre des éléments d'un rapport d'expertise précédent, dès lors que cette expertise effectuée sur l'élément en question n'est pas antérieure à 24 mois, qu'il est possible de prouver que l'élément sur lequel a porté cette expertise précédente n'a pas été modifié depuis et qu'aucune vulnérabilité sur cet élément n'a été révélée entre temps.

L'expertise portant sur une solution mise en œuvre pour un scrutin dont le niveau de risque est évalué à 2 peut reprendre des éléments d'un rapport d'expertise précédent, dès lors que cette expertise effectuée sur l'élément en question n'est pas antérieure à mois, qu'il est possible de prouver que l'élément sur lequel a porté l'expertise précédente n'a pas été modifié depuis et qu'aucune vulnérabilité sur cet élément n'a été révélée entre temps.

L'expertise portant sur une solution mise en œuvre pour un scrutin dont niveau de risque évalué à 3 doit être réalisée de nouveau, pour chaque élément, pour chaque élection.

L'expert ayant accès à des informations sensibles relatives aux solutions dont il est chargé d'évaluer la conformité, notamment le code source des applications, il est tenu de prendre toutes dispositions et précautions utilises afin de protéger les éléments qui sont portés à sa connaissance, notamment en limitant autant que possible les reproductions de code source au sein du rapport, en conservant ses rapports au sein d'espaces sécurisés dédiés et en ne conservant pas les éléments portés à sa connaissance au-delà de la durée nécessaire.

Le vote

Les heures d'ouverture et de fermeture du scrutin électronique doivent pouvoir être contrôlées par les membres du bureau de vote et les personnes désignées ou habilitées pour assurer le contrôle des opérations électorales.

Les fichiers nominatifs des électeurs constitués aux fins d'établir la liste électorale, d'adresser le matériel de vote et de réaliser les émargements ne peuvent être utilisés qu'aux fins précitées et ne peuvent être divulgués sous peine des sanctions pénales prévues par le code pénal.

La confidentialité des données est également opposable aux techniciens en charge de la gestion ou de la maintenance du système informatique.

Pour se connecter à distance ou sur place au système de vote, l'électeur doit s'authentifier conformément à la présente recommandation et à l'aide d'un moyen répondant à l'objectif de sécurité correspondant au niveau de risque identifié pour le scrutin. Au cours de cette procédure, le serveur de vote vérifie l'identité de l'électeur et que celui-ci est bien autorisé à voter. Dans ce cas, il accède aux listes ou aux candidats officiellement retenus et dans l'ordre officiel.

L'électeur doit pouvoir choisir une liste, un candidat ou un vote blanc de façon à ce que ce choix apparaisse clairement à l'écran, indépendamment de toute autre information. Il doit avoir la possibilité de revenir sur ce choix. Il valide ensuite son choix et cette opération déclenche l'envoi du bulletin de vote dématérialisé vers le serveur des votes. L'électeur reçoit alors la confirmation de son vote et dispose de la possibilité de conserver trace de cette confirmation. La solution de vote par correspondance électronique, notamment *via* Internet, doit proposer toutes les options offertes par les textes fondant le vote, le cas échéant le vote nul ou blanc.

Dans le cas où le scrutin est mixte, composé d'un vote par correspondance électronique associé à un vote par correspondance papier par exemple, il convient que le vote électronique permette aux électeurs les mêmes possibilités que celles offertes par le vote papier, telle que la possibilité de voter nul ou blanc lorsque cela est prévu pour un scrutin, afin de ne pas créer de distorsion en fonction du moyen utilisé. Dans le cas où ces différentes possibilités sont offertes à l'électeur, il convient d'être attentif au fait qu'une personne ne puisse pas voter deux fois, notamment en utilisant le système par correspondance papier et le système par Internet. Ainsi la solution retenue doit permettre d'écarter les votes par correspondance papier d'une personne ayant déjà voté par Internet.

Les garanties minimales pour un contrôle *a posteriori*

Pour des besoins d'audit externe, notamment en cas de contentieux électoral, le système de vote par correspondance électronique, notamment *via* Internet, doit pouvoir fournir les éléments techniques permettant au minimum de prouver de façon irréfutable que :

– le procédé de scellement est resté intègre durant le scrutin ;
– les clés de chiffrement/déchiffrement ne sont connues que de leurs seuls détenteurs ;
– le vote est anonyme lorsque la législation l'impose ;
– la liste d'émargement ne comprend que la liste des électeurs ayant voté ;
– l'urne dépouillée est bien celle contenant les suffrages des électeurs et qu'elle ne contient que ces suffrages ;
– aucun décompte partiel n'a pu être effectué durant le scrutin ;
– le dépouillement de l'urne peut être vérifié *a posteriori* et qu'il s'est déroulé de façon correcte.

La conservation des données portant sur l'opération électorale

Tous les fichiers supports (copies des codes sources et exécutables des programmes et du système sous-jacent, matériels de vote, fichiers d'émargement, de résultats, sauvegardes) doivent être conservés sous scellés jusqu'à l'épuisement des voies et délais de recours contentieux. Cette conservation doit être assurée sous le contrôle de la commission électorale dans des conditions garantissant le secret du vote. Obligation doit être faite au prestataire de service, le cas échéant, de transférer l'ensemble de ces supports à la personne ou au tiers nommément désigné pour assurer la conservation de ces supports. Lorsqu'aucune action contentieuse n'a été engagée à l'épuisement des délais de recours, il doit être procédé à la destruction de ces documents sous le contrôle de la commission électorale.

Dispositions transitoires et finales

La présente délibération est publiée au *Journal officiel* de la République française. Elle devra être prise en compte par les responsables de traitement après un délai transitoire de douze mois à compter de sa publication.

La présidente,
M.-L. Denis

Décrets, arrêtés, circulaires

TEXTES GÉNÉRAUX

MINISTÈRE DE L'EUROPE ET DES AFFAIRES ÉTRANGÈRES

Arrêté du 25 février 2021 portant création du registre de l'état civil centralisé dans le cadre de l'expérimentation de la dématérialisation des actes de l'état civil établis par le ministère de l'Europe et des affaires étrangères

NOR : *EAEF2104444A*

Le ministre de l'Europe et des affaires étrangères et le garde des sceaux, ministre de la justice,

Vu le règlement (UE) n° 910/2014 du Parlement européen et du Conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE ;

Vu le règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE ;

Vu le code civil, notamment ses articles 34 et suivants, et son article 1367 ;

Vu le code du patrimoine et notamment ses articles L. 213-1 et suivants ;

Vu la loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés ;

Vu l'ordonnance n° 2019-724 du 10 juillet 2019 relative à l'expérimentation de la dématérialisation des actes de l'état civil établis par le ministère des affaires étrangères ;

Vu le décret n° 2017-890 du 6 mai 2017 relatif à l'état civil ;

Vu le décret n° 2017-1416 du 28 septembre 2017 relatif à la signature électronique ;

Vu le décret n° 2019-993 du 26 septembre 2019 pris en application de l'ordonnance n° 2019-724 du 10 juillet 2019 relative à l'expérimentation de la dématérialisation des actes de l'état civil établis par le ministère des affaires étrangères,

Arrêtent :

Art. 1er. – Il est créé par le ministère des affaires étrangères, un traitement automatisé de données à caractère personnel dénommé « Registre d'état civil électronique » (RECE).

Ce traitement a pour finalité l'établissement, la gestion, la conservation et la délivrance des actes de l'état civil établis sous forme électronique par les autorités diplomatiques et consulaires ou par les officiers de l'état civil du service central d'état civil.

Le RECE est composé d'un registre électronique centralisé et d'un système de gestion des données de l'état civil.

Art. 2. – Les données à caractère personnel et les informations qui sont enregistrées et traitées dans le RECE prévu à l'article 1er du présent arrêté sont les suivantes :

1° Les données relatives au demandeur d'une copie intégrale ou d'un extrait d'acte de l'état civil : qualité (mandataire habilité, institutionnel particulier), type (si mandataire ou institution : nature de l'institution ou profession du mandataire), raison sociale ou titre (désignation du mandataire profession libérale ou SCP, Maitre), nom de naissance, nom d'usage, prénom(s), adresse postale, numéro de téléphone, adresse de courrier électronique, justificatif de qualité (décision judiciaire, carte professionnelle, pouvoir, mandat), motif de la demande ;

2° Les données relatives au ou aux titulaires de l'acte de l'état civil : nom(s), prénom(s), date et lieu de naissance, situation de famille, profession, sexe, filiation (nom, prénoms, date et lieu de naissance des parents, professions, sexe), décoration ;

3° Les données relatives aux tiers : déclarant, témoins, nom, prénom(s), date et lieu de naissance, profession, adresse postale, l'âge pour le déclarant, la qualité de majeur pour les témoins ;

4° Les données relatives à l'officier de l'état civil : nom, prénom(s), date de la signature et lieu d'exercice, certificat de signature électronique, image numérique de la signature, numéro d'identification, profil d'authentification, qualité, décoration ;

5° Les données relatives à l'évènement : naissance, mariage, décès, reconnaissance, enfant sans vie, date, heure et lieu de l'événement, contrat de mariage (date et lieu d'enregistrement) nom et prénom du professionnel ayant rédigé le contrat de mariage et son lieu d'exercice ;

6° Les données relatives aux mentions apposées en marge des actes de l'état civil.

Les données à caractère personnel mentionnées au présent article sont conservées pendant une durée de cent vingt ans dans le RECE à l'exception des données déclarées par le demandeur et relatives à une demande en délivrance d'une copie intégrale ou d'un extrait d'acte de l'état civil, qui sont conservées pendant douze mois.

Art. 3. – Les pièces nécessaires à l'établissement d'un acte de l'état civil seront conservées dans un format numérique pendant une durée de cinquante ans sous les réserves de l'article 7 de l'ordonnance n° 2019-724 du 10 juillet 2019 susvisée.

Les actes de l'état civil sont établis à partir des données indiquées à l'article 2 du présent arrêté. Ils seront conservés au format numérique signés électroniquement pendant une durée de cent vingt ans. Au-delà de cette date, les actes de l'état civil seront transférés sur le support d'archives numériques du ministère des affaires étrangères, SAPHIR (Système d'archivage pérenne pour l'histoire, l'information et la recherche).

Les copies intégrales ou les extraits d'actes de l'état civil sont établis à partir des données indiquées à l'article 2 du présent arrêté. Ils seront conservés au format numérique signés électroniquement pendant une durée de douze mois. Au-delà, ces documents seront détruits.

Art. 4. – La signature de l'officier de l'état civil est une signature électronique sécurisée utilisant un certificat numérique, procédé cryptographique visant à garantir l'intégrité du document signé et l'identité du signataire.

La signature électronique mise à la disposition des officiers de l'état civil est qualifiée au sens du règlement du Parlement européen et du Conseil du 23 juillet 2014 susvisé.

La signature électronique répond à un format PAdES.

Le certificat numérique sera délivré à l'officier de l'état civil sur support de carte à puce individuelle, remis en mains propres par un mandataire habilité, sur présentation d'une pièce d'identité.

La procédure d'inscription et d'enregistrement des données d'identification et d'habilitation de ces personnes est à l'initiative et sous la responsabilité du ministère des affaires étrangères.

Art. 5. – Les actes de l'état civil électroniques établis sont stockés sur le système d'archivage numérique, SAPHIR, implémentation au ministère des affaires étrangères de VITAM (valeurs immatérielles transmises aux archives pour mémoire), dupliqués d'un site principal vers un site distant.

L'intégrité des actes est assurée de manière pérenne par le système d'archivage qui trace et détecte toute intervention sur l'acte après scellement de l'acte au moment de son enregistrement.

Art. 6. – Le traitement automatisé de données à caractère personnel dénommé RECE est accessible par tous les officiers de l'état civil, à des fins d'établissement, de mise à jour et de délivrance, dans les limites de leur compétence territoriale telles que définies par les dispositions légales et réglementaires. Cette compétence est vérifiée au moyen d'un identifiant de l'officier de l'état civil associé à des droits portant sur une zone géographique précise.

L'accès au traitement automatisé par les officiers de l'état civil est contrôlé par un système d'authentification ministériel.

Ces attributions sont renseignées par une personne habilitée via un traitement de gestion des compétences dédié au RECE.

Le RECE est accessible à des fins de consultation à toute personne bénéficiant d'une autorisation conformément aux dispositions de l'article 26 du décret n° 2017-890 du 6 mai 2017 susvisé.

Le RECE assure la traçabilité des actions opérées par toutes personnes autorisées sur le traitement automatisé.

Art. 7. – Le présent arrêté sera publié au *Journal officiel* de la République française.

Fait le 25 février 2021.

Le ministre de l'Europe
et des affaires étrangères,
Pour le ministre et par délégation :
La directrice des Français à l'étranger
et de l'administration consulaire,
L. HAGUENAUER

Le garde des sceaux,
ministre de la justice,
Pour le ministre et par délégation :
La secrétaire générale
du ministère de la justice,
C. PIGNON

Texte 4

France Diplomatie

Les démarches d'état civil dématérialisées, nouvelle composante de l'administration numérique (15 mars 2021)

Ce vendredi 12 mars a marqué la première étape de la numérisation totale de démarches d'état civil relatives à des événements survenus à l'étranger concernant des ressortissants français. Il est dorénavant possible à ces usagers de demander et de recevoir des copies et extraits de leurs actes (naissance, mariage, décès) selon un procédé totalement dématérialisé.

C'est la loi du 10 août 2018 « pour un État au service d'une société de confiance » (loi ESSOC) qui est à l'origine de l'ambitieux projet RECE : Registre d'État Civil Électronique. Le pilotage, qui a été confié au MEAE (Direction des Français de l'étranger et de l'administration consulaire), s'articule selon trois principaux objectifs : un service plus rapide, plus accessible et de qualité accrue pour les usagers, un recentrage sur l'expertise juridique des officiers d'état civil dégagés de multiples contraintes techniques, des économies pour l'État tirées de la forte réduction des coûts d'impression et d'envoi des actes papier.

Un impératif de sécurité, notamment en matière de fraude, a par ailleurs déterminé des choix numériques permettant de garantir la protection des données des usagers et l'authenticité des actes d'état civil produits. Ceux-ci, reçus et conservés par le demandeur dans son espace personnel qu'il aura créé au sein du portail service-public.fr, pourront être acheminés vers les entités qui les ont requis (administrations, organismes sociaux, ...) par des canaux fortement sécurisés. Au cas où une version imprimée serait demandée à l'usager, un téléservice de vérification des informations a été développé, permettant aux entités destinataires de s'assurer que le document présenté est bien conforme au document authentique.

Avec France Consulaire et le vote par internet portés également par la DFAE, le RECE est l'un des trois projets stratégiques du ministère de l'Europe et des affaires étrangères dans l'ensemble des réalisations du gouvernement pour améliorer la vie des citoyens. Les prochaines étapes du RECE consisteront notamment en une refonte approfondie du système de traitement du service central de l'état civil (SCEC) et, progrès substantiel pour les administrés, de la possibilité de déclarer en ligne naissances et mariages.

Décrets, arrêtés, circulaires

TEXTES GÉNÉRAUX

MINISTÈRE DE L'EUROPE ET DES AFFAIRES ÉTRANGÈRES

Décret n° 2023-998 du 27 octobre 2023 portant expérimentation de la procédure dématérialisée de demande de renouvellement d'un passeport

NOR : *EAEF2310407D*

Publics concernés : *citoyens français, administrations.*

Objet : *expérimentation portant sur le renouvellement, pour les ressortissants français majeurs résidant au Canada ou au Portugal inscrits au registre des Français établis hors de France, d'un passeport sans comparution personnelle du demandeur au moment du dépôt de la demande, avec remise du titre par envoi postal sécurisé.*

Entrée en vigueur : *le décret entre en vigueur le lendemain de sa publication, mais l'expérimentation débute à compter du 1er mars 2024.*

Notice : *l'expérimentation concerne l'ensemble des Français majeurs résidant au Canada et au Portugal souhaitant déposer une demande de renouvellement d'un passeport obtenu après leur majorité. L'expérimentation vise à faciliter les démarches administratives des Français de l'étranger, dont les déplacements auprès des ambassades et consulats sont parfois longs et coûteux. Cette expérimentation débute à compter du 1er mars 2024 et prend fin le 28 février 2025.*

Références : *les décrets qu'il modifie, dans leur rédaction résultant de cette modification, peuvent être consultés sur le site Légifrance (https://www.legifrance.gouv.fr).*

La Première ministre,

Sur le rapport du ministre de l'intérieur et des outre-mer et de la ministre de l'Europe et des affaires étrangères,

Vu la Constitution, notamment son article 37-1 ;

Vu le règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016, relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE ;

Vu le règlement (CE) n° 2252/2004 du Conseil du 13 décembre 2004 établissant des normes pour les éléments de sécurité et les éléments biométriques intégrés dans les passeports et les documents de voyage délivrés par les Etats membres ;

Vu le code général des impôts, notamment son article 953 ;

Vu le code civil, notamment ses articles 60, 61 et 61-3-1 ;

Vu la loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés, notamment son article 32 ;

Vu la loi n° 2022-301 du 2 mars 2022 relative au choix du nom issu de la filiation ;

Vu le décret n° 81-778 du 13 août 1981 modifié fixant le tarif des droits à percevoir dans les chancelleries diplomatiques et consulaires et, en territoire français, par le ministère des relations extérieures ;

Vu le décret n° 2003-1377 du 31 décembre 2003 modifié relatif à l'inscription au registre des Français établis hors de France ;

Vu le décret n° 2004-1543 du 30 décembre 2004 modifié relatif aux attributions des chefs de poste consulaire ;

Vu le décret n° 2005-1726 du 30 décembre 2005 modifié relatif aux passeports ;

Vu le décret n° 2016-1460 du 28 octobre 2016 modifié autorisant la création d'un traitement de données à caractère personnel relatif aux passeports et aux cartes nationales d'identité ;

Vu l'avis n° 2023-077 de la Commission nationale de l'informatique et des libertés en date du 20 juillet 2023 ;

Le Conseil d'Etat (section de l'intérieur) entendu,

Décrète :

Art. 1er. – A titre expérimental, à compter du 1er mars 2024 et jusqu'au 28 février 2025, les ressortissants français majeurs ayant leur résidence habituelle au Canada ou au Portugal et inscrits au registre des Français établis hors de France peuvent, dans les conditions prévues à l'article 2, demander le renouvellement d'un passeport dans le cadre d'une procédure dématérialisée.

Cette procédure fait l'objet d'un arrêté du ministre chargé des affaires étrangères précisant notamment les modalités de la vérification à distance de l'identité du demandeur, en particulier au moyen de son authentification sur le registre des Français établis hors de France et d'un rendez-vous en visio-conférence lors duquel le demandeur présente le passeport dont il sollicite le renouvellement, les conditions du télépaiement des droits de chancellerie, ainsi que celles dans lesquelles les titres délivrés sont adressés au demandeur par courrier sécurisé.

Sont exclus du champ de l'expérimentation :

– les renouvellements pour perte ou vol ;
– les renouvellements pour changement de prénom ou de nom demandé sur le fondement des articles 60, 61 et 61-3-1 du code civil ;
– les demandes de second passeport ;
– les renouvellements de passeports ayant déjà fait l'objet du dispositif prévu par la présente expérimentation, à l'exception de ceux résultant d'une erreur imputable à l'administration ;
– les renouvellements de passeports des usagers qui n'avaient pas pu fournir leurs empreintes digitales en raison de circonstances particulières au moment du dépôt de leur demande ;
– les renouvellements de passeports expirés depuis plus de cinq ans à la date de la demande ;
– les renouvellements de passeports délivrés avant la majorité du titulaire.

Art. 2. – Par dérogation au I de l'article 5-1 du décret du 30 décembre 2005 susvisé, la condition tenant à la production d'une des pièces qui y sont mentionnées est satisfaite par celle d'une copie.

Par dérogation à l'article 6 du décret du 30 décembre 2005 susvisé, les documents par lesquels le demandeur justifie de sa résidence datent de moins d'un mois.

Par dérogation à l'article 6-1 du décret du 30 décembre 2005 susvisé, il n'est pas procédé au recueil des empreintes digitales lors du dépôt de la demande.

Par dérogation au I de l'article 9 du décret du 28 octobre 2016 susvisé, la durée de conservation de l'image numérisée des empreintes digitales prises lors du dépôt de la demande du titre dont il est obtenu le renouvellement dans le cadre de la présente expérimentation est portée de 15 à 25 ans.

Art. 3. – La mise en œuvre de l'expérimentation fait l'objet d'un rapport d'évaluation, remis aux ministres chargés de l'intérieur et des affaires étrangères au plus tard trois mois avant son terme, établi par un comité, dont la composition est prévue par un arrêté de ces deux ministres, comprenant des membres de l'inspection générale de l'administration du ministère de l'intérieur et de l'inspection générale des affaires étrangères, des personnalités qualifiées ainsi que des représentants des usagers.

Ce rapport porte notamment sur :

– le nombre de demandes de recours à ce dispositif ;
– l'impact sur les demandes de titres ;
– les délais de délivrance des passeports ;
– les éventuelles difficultés rencontrées, en particulier les tentatives de fraude et d'usurpation d'identité ;
– les éléments spécifiques à la vérification d'identité à distance, concernant tant la sécurité des systèmes d'information que la fiabilité de la vérification ;
– l'évolution du coût financier et en personnel pour les ministères chargés des affaires étrangères et de l'intérieur ainsi que pour l'Agence nationale des titres sécurisés ;
– la mise en œuvre de la solution de télépaiement destinée à permettre aux usagers de régler par ce biais les droits exigés pour le renouvellement du passeport ;
– le degré de satisfaction et de confiance du public ayant recouru à la procédure dématérialisée.

Art. 4. – Le ministre de l'intérieur et des outre-mer et la ministre de l'Europe et des affaires étrangères sont chargés, chacun en ce qui le concerne, de l'exécution du présent décret, qui sera publié au *Journal officiel* de la République française.

Fait le 27 octobre 2023.

ÉLISABETH BORNE

Par la Première ministre :

La ministre de l'Europe et des affaires étrangères,
CATHERINE COLONNA

Le ministre de l'intérieur et des outre-mer,
GÉRALD DARMANIN

Texte 6

https://www.diplomatie.gouv.fr/fr/services-aux-francais/voter-a-l-etranger/foire-aux-questions/

Foire aux Questions – Voter à l'étranger (extraits)

24. Comment puis-je vérifier que mon bulletin a bien été pris en compte dans le calcul des résultats (vérifiabilité individuelle) ?

Il faut attendre plusieurs jours après le dépouillement des votes.

Conformément à l'objectif de sécurité n° 3-02 (« *permettre la transparence de l'urne pour tous les électeurs à partir d'outils tiers* ») de la délibération de la CNIL n° 2019-053 du 25 avril 2019, le MEAE a sollicité le Centre national de la recherche scientifique (CNRS) pour développer un outil permettant à chaque électeur de vérifier, après le dépouillement de l'urne électronique, que son bulletin a bien été pris en compte dans le calcul des résultats.

25. Comment m'assurer que mon vote est sécurisé ?

Outre les différents tests d'intrusion menés sur la plateforme, la solution de vote a fait l'objet de différents audits de sécurité réalisés sur son architecture et son code source. Ces audits, ainsi que l'analyse de risques ayant permis d'apprécier les risques relatifs à la sécurité selon les préconisations de l'Agence nationale de la sécurité des systèmes d'information (ANSSI), ont montré que cette solution de vote satisfaisait aux exigences techniques de fiabilité.

Par ailleurs, le système de vote est homologué en mars 2023, après avis positif d'une commission composée de représentants du MEAE, du ministère de l'Intérieur, de l'ANSSI et du Bureau du vote électronique.

26. Mon vote est-il anonyme et secret ?

Comme les autres modalités de vote proposées, le vote par internet garantit le secret et l'anonymat de votre vote.

La confidentialité du vote est protégée dès la création du bulletin.

Le bulletin de vote n'est jamais lisible lors de sa transmission vers l'urne électronique : il ne circule que sous une forme chiffrée. De la même façon, il est stocké au sein de l'urne uniquement sous forme chiffrée.

Il n'est pas possible de relier l'identité d'un électeur à son bulletin de vote : le bulletin de vote est anonyme, et les bulletins unitaires ne sont donc jamais déchiffrés, **seule l'accumulation des bulletins chiffrés est déchiffrée**, ce qui protège encore davantage le secret du vote.

L'accumulation des bulletins de vote ne peut être déchiffrée qu'au moment du dépouillement : la clé de déchiffrement n'est accessible qu'avec la participation d'un nombre minimum de membres du Bureau du vote électronique, et il est procédé au dépouillement à partir d'un système déconnecté d'internet.

27. Quelles sont les garanties quant au bon déroulement des opérations électorales et à l'effectivité des dispositifs de sécurité ?

Le Bureau du vote électronique veille au bon déroulement des opérations électorales et vérifie l'effectivité des dispositifs de sécurité prévus pour assurer le secret du vote, la sincérité du scrutin, et l'accessibilité au suffrage (alinéa 1er de l'article R. 176-3-3 du code électoral).

Il peut, à tout moment, s'assurer de l'intégrité et de la disponibilité du système de vote et des fichiers prévus au deuxième alinéa de l'article R. 176-3 du code électoral. Par ailleurs, il est compétent pour prendre toute mesure d'information et de sauvegarde, y compris l'arrêt

temporaire ou définitif des opérations de vote par voie électronique s'il estime que leur sincérité, leur secret ou leur accessibilité n'est plus garanti (article R. 176- 3-3 du code électoral).

Le Bureau du vote électronique est composé (article R. 176-3-1 du code électoral) :

- D'un membre du Conseil d'Etat ou de son suppléant
- De la directrice des Français à l'étranger et de l'administration consulaire au ministère de l'Europe et des Affaires étrangères ou de son suppléant ;
- Du directeur du numérique au ministère de l'Europe et des Affaires étrangères ou de son suppléant ;
- Du directeur de la modernisation et de l'administration territoriale au ministère de l'intérieur ou de son suppléant ;
- Du directeur de l'Agence nationale de la sécurité des systèmes d'information ou de son suppléant ;
- De la présidente de l'Assemblée des Français de l'étranger et de ses deux vice-présidents ou de leurs suppléants.

28. Lesquelles de mes données personnelles sont utilisées pour le vote par internet et comment sont-elles protégées ?

Dans le cadre du vote par internet, vos données personnelles sont extraites soit du Registre des Français établis hors de France (données communiquées via le Registre en ligne, ou au guichet consulaire), soit du répertoire des électeurs sur lequel vous êtes inscrit(e), puis intégrées à la plateforme de vote.

Les données des électeurs collectées sont les suivantes : nom, prénom(s), lieu de résidence, adresse électronique, numéro d'inscription au Registre (NUMIC) ou au répertoire des électeurs (NUMEL), ainsi que numéro de téléphone portable. Le numéro d'inscription au Registre est également appelé numéro d'identification consulaire.

Le système de vote collecte également les informations suivantes de l'électeur :

- l'expression de son vote ;
- les données relatives à son émargement ;
- son adresse IP ;
- la version de son navigateur ;
- les traceurs (cookies) nécessaires au fonctionnement du portail de vote.

Les données des candidats collectées sont les suivantes : nom, prénom(s), circonscription électorale, et, le cas échéant l'étiquette politique, telle que renseignée sur la déclaration de candidature. Cette étiquette politique ne peut excéder 150 caractères, espaces compris.

La présente Foire aux Questions précise les conditions dans lesquelles la Direction des Français à l'étranger et de l'administration consulaire (DFAE) du Ministère de l'Europe et des Affaires étrangères, dont le siège est situé au 37 Quai d'Orsay, 75007, Paris, traite les données personnelles en sa qualité de responsable du traitement (au sens du point 7 de l'article 4 du Règlement (UE) 2016/679 du 27 avril 2016, rendu applicable sur renvoi du 3ème alinéa de l'article 2 de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés).

Pour de plus amples informations à ce sujet, vous pouvez consulter les Mentions légales de la plateforme de vote par internet.

L'hébergement des données est assuré par le Ministère de l'Europe et des Affaires étrangères dont les serveurs sont situés en France.

29. Quel usage est fait de mes données et sur quelle base légale sont-elles traitées ?

Le traitement de l'ensemble des données décrites dans le point précédent a pour seule et unique finalité de permettre la mise en œuvre du vote par internet pour l'élection des députés des Français établis hors de France, au moyen de matériels et de logiciels de nature à respecter le secret du vote et la sincérité du scrutin.

Ce traitement est nécessaire à l'exécution d'une mission d'intérêt public, à savoir l'organisation de scrutins à l'étranger, et à l'accessibilité des électeurs Français établis hors de France au suffrage qui en découle, au même titre qu'un Français résidant sur le territoire national.

Le traitement de vos données à caractère personnel répond par ailleurs au respect d'une obligation légale (Ordonnance n° 2009-936 du 29 juillet 2009 relative à l'élection de députés par les Français établis hors de France).

Vos données personnelles ne seront pas utilisées pour d'autres finalités que l'élection des députés des Français établis hors de France de mars et avril 2023.

30. Qui a accès à mes données personnelles ?

Seuls les agents habilités de la Direction des Français à l'étranger et de l'administration consulaire (DFAE) du Ministère de l'Europe et des Affaires étrangères et le personnel habilité des sous-traitants qui mettent en œuvre le vote par internet pour son compte ont accès, en raison de leurs attributions légales et dans la limite du besoin d'en connaître, à tout ou partie de vos données personnelles.

31. Combien de temps mes données personnelles sont-elles conservées ?

Vos données personnelles sont détruites dans les délais énoncés à l'article R. 179-1 du code électoral et à l'article 33 de l'ordonnance n°58-1067 du 7 novembre 1958.

Le délai de conservation est en principe de 10 jours à compter de la proclamation des résultats de chaque tour.

L'article R. 179-1 du code électoral prévoit des exceptions à ce délai. Pour plus d'informations veuillez consulter la page « Mentions légales ».

32. Mes données sont-elles transférées en dehors de l'Union Européenne ?

Aucune de vos données à caractère personnel n'est transmise à des instances hors de l'Union Européenne.

33. Quels sont les droits dont je bénéficie sur mes données personnelles ?

Conformément à l'article R. 176-3 du code électoral, le traitement n'entre pas dans le champ d'application du règlement (UE) 2016/679 du 27 avril 2016.

Vous bénéficiez des garanties offertes par le titre Ier de la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, les articles 49 et 50 du titre II, et de l'information prévue à l'article 48 de la même loi.

Conformément à l'article R. 176-3 du code électoral, vous pouvez exercer vos droits d'accès et de rectification auprès du ministre des affaires étrangères. Les informations de contact sont précisées au point 35.

34. Puis-je m'opposer au traitement de mes données personnelles ?

En application de l'article R. 176-3 du code électoral, vous ne pouvez pas vous opposer au traitement de vos données personnelles pour la mise en œuvre du vote par internet.

35. Comment puis-je exercer mes droits en matière de protection de données personnelles ?

Pour exercer vos droits d'accès ou de rectification ou pour toute question sur le traitement des données personnelles mis en œuvre par le Ministère de l'Europe et des Affaires étrangères, vous pouvez contacter son délégué à la protection des données :

- Par courrier : Délégué général à la protection des données (DPO), au 27 rue de la Convention – 75732 PARIS cedex 15 ;
- Par courriel : Au DPO (droits-rgpd.meae@diplomatie.gouv.fr) ;

Si vous estimez, après l'avoir contacté, que vos droits ne sont pas respectés ou que ce dispositif n'est pas conforme aux règles en matière de protection des données, vous pouvez adresser une réclamation auprès de la Commission nationale de l'informatique et des libertés (CNIL).

Texte 7

https://www.latribune.fr/opinions/tribunes/les-francais-sont-ils-prets-pour-le-vote-par-internet-964673.html

Les Français sont-ils prêts pour le vote par internet ?

OPINION. Le vote en ligne est souvent évoqué depuis quelques années, notamment pour lutter contre l'abstention de plus en plus forte. La crise sanitaire et la montée de l'abstention ont poussé des personnalités politiques à se prononcer en sa faveur. Tour d'horizon d'un véritable enjeu démocratique.
Par Jérôme de Forsan de Gabriac, consultant sénior Sopra Steria Next ; Margot Maufroy, étudiante en master Cybersecurity and Defense Management EM Lyon et Boris Laurent, manager Défense & Sécurité Sopra Steria Next.
Jérôme de Forsan de Gabriac, Margot Maufroy et Boris Laurent

05 Juin 2023, 12:00

En France, il existe plusieurs moyens de voter : dans un bureau de vote, en ligne sur internet et par procuration (1). Aujourd'hui, les alternatives au déplacement dans le bureau de vote sont utilisées dans des cas très spécifiques. Le vote par internet, lors des élections consulaires et législatives pour les Français de l'étranger, en est un (2).

Le vote en ligne est largement adopté

Le second tour des élections législatives s'est tenu les 15 et 16 avril 2023 dans les 2e, 8e et 9e circonscriptions des Français établis hors de France. L'analyse des résultats disponibles sur le portail internet France Diplomatie montre une forte adoption du vote par internet.

	2ème circonscription	8ème circonscription	9ème circonscription	TOTAL	Ratio
Total vote à l'urne	2 795	3 677	4 149	10 621	**27%**
Total vote par correspondance	2	15	3	20	0%
Total vote par internet	7 163	12 652	8 759	28 574	**73%**
TOTAL	9 960	16 344	12 911	39 215	100%

Un phénomène qui vient d'ailleurs confirmer une tendance. En effet, lors des élections législatives de juin 2022, sur la totalité des 11 circonscriptions représentant près d'un million et demi d'inscrits, le taux de vote par internet avait atteint un pic de 75%. Probablement « boosté » par la période covid, le vote par internet semble néanmoins être une méthode de plus en plus populaire pour exprimer son choix électoral. Pratique, confortable (3), il permet aux électeurs de voter de n'importe quel endroit, à tout moment, même de manière anticipée, et sans avoir à se déplacer dans un bureau de vote. Notons que pour l'heure, les différentes expérimentations n'ont pas démontré que le vote en ligne fait augmenter le taux de participation, mais cela pourrait évoluer dans le temps.

Mais de nombreuses questions et inquiétudes subsistent

Cependant, le vote en ligne soulève de nombreuses questions et inquiétudes comme la transparence du système, les erreurs et les pannes ou encore le piratage et les cyberattaques.

Actuellement, la transparence des systèmes de vote électronique concerne notamment l'accès public à des informations clés, des documents (code source, rapports, etc.) et l'observation de tests.Mais d'une manière plus générale, le vote électronique impose un paradoxe entre d'une part l'anonymat, et d'autre part la transparence. Le fait que le bulletin de vote tombe dans une urne transparente n'est pas dû au hasard. Dès lors, comment vérifier que le vote par internet est un système totalement clair et sûr ?

D'autre part, le « secret du vote », c'est-à-dire la confidentialité et l'anonymat dans l'urne qui empêchent le risque de votes sous la contrainte, ne peut pas être vérifié avec le vote en ligne. Le respect de la vie privée est aussi un enjeu capital car seul l'électeur doit savoir pour qui il a voté.

Enfin, le vote par internet est par nature plus sensible aux erreurs ou pannes potentiellement de grande ampleur, voire de cyberattaques et de piratage (4). À ce titre, lors des élections législatives de juin 2022, le Conseil constitutionnel a annulé les opérations électorales dans deux circonscriptions des Français établis hors de France en raison de disfonctionnements techniques (5).

Pour ces raisons, le maintien du bureau de vote est indispensable

Le système de vote ne doit pas être une entrave à l'expression des convictions politiques des personnes âgées, en situation de handicap, en difficulté avec le numérique ou ne disposant pas d'un terminal moderne. On notera à cet égard que l'assistance des votants par des aidants n'est pas compatible avec le principe de confidentialité.

D'une manière plus large, selon une étude INSEE publiée en 2022, les contraintes liées à la dématérialisation ont dissuadé les personnes les plus vulnérables de mener à bien des procédures sur internet. Ainsi, 32% des majeurs ont renoncé au moins une fois à une démarche en ligne pendant les 12 derniers mois. Parmi eux, les trois quarts l'ont effectuée par d'autres moyens (par téléphone, sur place, etc.) ; les autres (8% de la population totale) y ont renoncé définitivement. Dans ces conditions, le maintien des bureaux de vote parait donc indispensable ; le bureau de vote n'est pas une variable d'ajustement servant à financer le dispositif de vote par internet ; s'y déplacer est par ailleurs un rituel républicain fort.

Ailleurs dans le monde : l'Estonie à la pointe du eVoting

Dans le monde et en Europe, le vote en ligne connait des situations variables. L'État de la Nouvelle-Galles du Sud en Australie l'autorise notamment pour les élections législatives. Au Canada, un grand nombre de villes des provinces de l'Ontario, de la Nouvelle-Écosse et des Territoires du Nord-Ouest et du Yukon utilisent le vote par internet pour les élections municipales. De son côté, le Québec va lancer un projet pilote pour permettre aux électeurs de voter en ligne lors des élections municipales de 2025.

En Europe, La Norvège a suspendu l'utilisation du vote par internet et l'Allemagne l'a déclaré inconstitutionnel. En Belgique, un rapport a souligné la complexité technique du vote en ligne mais Bruxelles espère le rendre opérationnel à l'horizon 2034.En Suisse, après l'arrêt du vote en ligne en 2019, le Conseil fédéral a accordé aux cantons de Bâle-Ville, de Saint-Gall et de Thurgovie, l'autorisation de voter en ligne pour la votation fédérale du 18 juin 2023.

Mais c'est sans conteste l'Estonie qui est devenue la « championne » du eVoting. En effet, ce pays propose, en complément du scrutin physique, le vote par internet pour toutes ses élections. La part des votes en ligne est ainsi passée de 5,5% des participants aux législatives de 2007, à 43,8% en 2019. C'est également le seul État membre de l'Union à avoir utilisé ce type de vote lors des dernières élections européennes (2019), avec un record de 46,7% de votants en ligne. L'État estonien est en outre très transparent dans la mesure où il rend public le code source de son système. Comment expliquer un tel succès ?

« *L'identité électronique estonienne est disponible depuis 2002, mais n'a pas décollé immédiatement. Au départ, il n'y avait pas beaucoup de services électroniques que vous pouviez utiliser avec cette carte d'identité. D'un autre côté, les fournisseurs de service n'étaient pas intéressés par le développement d'accès électroniques car peu de personnes disposaient d'une telle carte. C'était en quelque sorte le problème de l'œuf ou de la poule. Mais en 2005, le vote électronique s'est révélé être une application à grand succès et beaucoup de gens ont demandé leur carte d'identité numérique pour pouvoir voter*

électroniquement », explique Jan Willemson, senior researcher chez Cybernetica (société qui a développé le système de vote électronique en Finlande), interrogé par Jérôme de Forsan de Gabriac.

Au début des années 2000, l'Estonie a lancé une carte d'identité numérique servant à la fois pour l'identité civile et pour l'authentification, notamment pour le vote en ligne. Les Estoniens utilisent cette carte pour accéder à un grand nombre de services numériques gouvernementaux et privés (impôts, dossier médical, résultats scolaires des enfants, prêt de livres à la bibliothèque, etc.). Dans ce contexte, c'est bien l'identité numérique qui est incontestablement le facteur clé du succès estonien.

Il est important de rappeler que les élections sont l'un des fondements de la démocratie et qu'elles doivent être protégées contre toute forme de fraude ou de manipulation. Aussi, une identité numérique régalienne, s'appuyant sur la délivrance en mairie d'un titre hautement sécurisé, et s'inscrivant dans un schéma européen favorisant une adoption via de nombreux usages, est de nature à apporter cette protection, alors que deux tiers des Français affirment être favorables au vote par internet.

_____

(1) La procuration fait son apparition en France en 1975, pour remplacer le vote par correspondance, alors interdit suite à des fraudes diffuses dans l'ensemble du territoire. Aujourd'hui, seuls les Français de l'étranger et les personnes incarcérées peuvent voter par correspondance.

(2) Les électeurs reçoivent leurs codes d'authentification par mail et par SMS. Le système utilisé est certifié par l'Agence nationale de la sécurité des systèmes d'information (ANSSI).

(3) Selon l'enquête post-électorale en ligne People 2022, ESPOL/CERAPS/LEM, septembre 2022, Version 1.0

(4) En 2017, les Français de l'étranger n'ont pas pu voter par internet lors des élections législatives de juin, en raison d'une menace élevée de cyberattaque.

(5) En Algérie (9e circonscription) et en Argentine (2e circonscription), le taux de délivrance des mots de passe aux électeurs inscrits ayant communiqué leurs coordonnées n'a été que de 38 %. Le Conseil constitutionnel a également annulé des élections dans la 8e circonscription (bassin Est de la Méditerranée). L'administration consulaire devait transmettre les adresses mail et les numéros de téléphone des citoyens inscrits sur les listes électorales consulaires. Mais suite à une erreur, c'est un autre fichier qui a été transmis.

Jérôme de Forsan de Gabriac, Margot Maufroy et Boris Laurent

Texte 8

https://www.inria.fr/fr/vote-electronique-securite-numerique-confidentialite

Sécurisation du vote électronique : des failles et des solutions

Mis à jour le *29/08/2023*

À l'heure du tout numérique, la sécurisation des échanges d'informations revêt une importance capitale, surtout pour le vote électronique. Après avoir identifié des vulnérabilités dans le protocole mis en place pour les élections législatives en France de juin 2022, Alexandre Debant et Lucca Hirschi, chercheurs Inria dans l'équipe Pesto (commune à Inria et au Loria), ont proposé des solutions d'amélioration prises en compte avec succès dès le scrutin suivant.

Lors des élections législatives de 2022, les ressortissants français résidant à l'étranger ont eu recours au **vote électronique à distance**. Si cette solution offre de nombreux avantages en termes d'organisation et d'accessibilité, elle nécessite toutefois la mise en place d'un protocole offrant les mêmes garanties de sécurité et de confidentialité que celles d'un bureau de vote traditionnel. *« Pour les législatives de 2017, il n'y avait pas eu de vote par Internet car l'ANSSI (Agence nationale de sécurité des systèmes d'information) estimait que le système proposé à l'époque n'atteignait pas un degré de sécurité suffisant »*, rappelle Alexandre Debant. *« L'ANSSI émet un avis consultatif qui est généralement suivi par les autorités en charge de l'organisation des scrutins,* complète Lucca Hirschi. *En 2022, l'enjeu était d'importance puisque, si l'on tient compte du nombre de bulletins transmis, il s'agit de la plus grosse élection par voie électronique jamais organisée à l'échelle mondiale. Cette année, l'ANSSI avait donné son feu vert après audit. »*

Les deux chargés de recherche se sont donc intéressés de près à l'opération. *« Nos collègues Véronique Cortier, Pierrick Gaudry et Stéphane Glondu, qui développent la plate-forme de vote Belenios, ont été chargés de mettre en place un **outil de vérification "tiers de confiance"** lors de ces élections,* expliquent-ils. *De façon indépendante, nous nous sommes spontanément saisis de la question et avons voulu étudier **les limites des mécanismes de défense**. Un mois avant le scrutin, un document de présentation du protocole a été publié et dès la première lecture nous avons soupçonné **des failles de sécurité** potentielles. L'examen du **code du programme** n'a fait que confirmer nos craintes de la vacuité de l'outil de vérification tiers de confiance. »*

Des garanties de sincérité et de secret du vote électronique

Dans un bureau de vote classique, la présence physique de l'électeur, qui dépose lui-même son bulletin dans une urne transparente, et celle des assesseurs, qui enregistrent le vote et procèdent à l'ouverture publique des urnes, assurent la sincérité du scrutin. *« On distingue en général deux types de **garanties de sécurité**. La première est la **confidentialité du vote**. Concrètement : personne ne doit savoir pour qui j'ai voté. La seconde concerne **l'intégrité du résultat** : le résultat proclamé doit correspondre à la somme de tous les bulletins envoyés (aucun bulletin n'a été modifié ou supprimé) et ces bulletins doivent avoir été envoyés par des votants légitimes. Avec le vote électronique, on cherche à atteindre les mêmes niveaux de sécurité que dans un vote papier grâce à la cryptographie. »*

Lors de l'envoi d'un bulletin pendant les législatives de 2022, chaque votant se voyait adresser un reçu – au format PDF – composé de données cryptographiques, lui permettant de vérifier la bonne prise en compte de son vote, soit sur le site du ministère de l'Europe et des Affaires étrangères (MEAE), soit sur celui créé par le tiers de confiance mandaté par le MEAE. Quant

au secret du vote, il était assuré par une clé de déchiffrement répartie entre les seize personnes constituant le bureau de vote électronique, notamment un membre du Conseil d'État, le directeur de l'ANSSI, des personnels du ministère et des membres de l'Assemblée des Français de l'étranger. C'est dans le principe de fonctionnement du protocole et dans sa conception qu'Alexandre Debant et Lucca Hirschi ont décelé des vulnérabilités menant à des attaques sur la vérifiabilité comme sur le secret du vote.

Vulnérabilités dans le protocole et le code

« En ce qui concerne la vérifiabilité du vote, nous avons ***décelé un problème dans l'implémentation du programme notamment dû à un*** **bug***. Au moment où le votant crée son bulletin de vote, son ordinateur le chiffre avec la clé du bureau et calcule une empreinte unique à ce bulletin. Le bulletin est transmis au serveur qui calcule de son côté un reçu devant contenir, entre autres choses, cette empreinte. »*

« Ce reçu est envoyé sous plusieurs formes puis affiché au votant. La logique voudrait que l'ordinateur du votant vérifie la consistance du reçu avec l'empreinte préalablement calculée avant de l'afficher, mais quand nous avons analysé le code, nous avons constaté qu'il y avait une faille à ce stade : cette vérification n'était pas complète et il était possible de la tromper. » Une compromission du serveur rendait donc possible une modification du bulletin envoyé tout en adressant au votant un reçu qui laisserait penser à celui-ci que son vote a été enregistré conformément à son choix. La vérifiabilité est donc cassée ainsi que l'intégrité et la sincérité du scrutin.

« ***Pour le secret du vote, l'attaque exploite une autre faiblesse, non plus du code mais du protocole en lui-même.*** *Sur le plan électoral, les Français de l'étranger sont répartis selon onze zones découpées elles-mêmes en circonscriptions consulaires qui correspondent chacune à un bureau de vote. Toutes ces circonscriptions ne sont pas de taille égale. À Sydney par exemple, il y a des dizaines de milliers de votants qui se sont exprimés alors qu'à Ekaterinbourg, il y en a eu moins de dix.* ***Nous avons découvert qu'il était possible, pour un attaquant, de cibler un votant, de détourner son bulletin vers une circonscription consulaire où il y a très peu de votes, voire pas du tout, et de savoir ainsi, au dépouillement, pour qui il a voté. Cela est rendu possible par une faille dans la conception des preuves à divulgation nulle de connaissance qui accompagnent les bulletins.*** *»* Ainsi, l'autre objectif central du protocole, la confidentialité du vote, est également compromis.

De l'ENS à Inria

Après des études à l'École normale supérieure de Rennes, **Alexandre Debant** a soutenu sa thèse à l'IRISA (Institut de recherche en informatique et systèmes aléatoires) puis, en septembre 2020, a intégré en postdoc le Centre Inria de Nancy, où il a été recruté en tant que chargé de recherche deux ans plus tard.

Originaire de Suisse romande, **Lucca Hirschi** a quant à lui poursuivi sa thèse à l'École normale supérieure de Cachan avant d'intégrer l'École polytechnique fédérale (ETH) de Zurich en postdoctorat et de rejoindre Inria en tant que chargé de recherche en janvier 2019.

Une démarche constructive

*« Nous avons montré que, selon le modèle d'attaquant, il peut y avoir des attaques qui permettent à un tel attaquant de tricher****. Nous ne pouvons pas dire si l'élection de 2022 a subi de telles attaques. En effet, nous avons montré qu'elles n'auraient laissé aucune trace détectable, même*** **via** ***une investigation*** **a posteriori.** *La notion de modèle d'attaquant est très importante parce qu'elle définit la nature des attaques potentielles****. Les vulnérabilités et attaques que nous avons révélées sont exploitables par un attaquant qui compromettrait soit***

le serveur de vote administré par le MEAE, soit le canal sécurisé transportant les communications (TLS). *Dans le cadre d'une élection d'une telle ampleur, de tels scénarios doivent être pris en compte (ce que recommande d'ailleurs la CNIL, voir son niveau 3 de sécurité). En pratique, le serveur de vote pourrait être compromis suite à une négligence humaine, un acte malveillant ou un* bug*, et le canal sécurisé peut être compromis par une architecture défaillante ou compromise au point d'entrée (c'est-à-dire réseau professionnel) ou au point d'arrivée (serveur de vote administré par le MEAE).* ***D'un point de vue sociétal, cela pose plus largement la question d'une élection nationale dont la sincérité repose entièrement sur la confiance d'une seule entité, qui plus est étatique*** *(le MEAE). À l'opposé, le vote papier répartit la confiance notamment entre les différents bureaux de vote et assesseurs. D'un point de vue purement technique, on rappelle que tout l'objectif de la vérifiabilité et du reçu cryptographique est précisément d'éviter de devoir faire confiance à une telle autorité centralisée. »*

Le passage de la théorie à la pratique est l'une de nos préoccupations essentielles.

Le travail d'Alexandre Debant et Lucca Hirschi ne se limite pas à pointer les faiblesses d'un système mais vise à **proposer des solutions d'amélioration**. Après échanges avec le ministère (MEAE), l'ANSSI et la société *Voxaly Docaposte*, fournisseur de l'outil de vote, ils ont fait **six propositions de contre-mesures pour réparer et renforcer la sécurité du protocole établi.** *« L'idée est d'être toujours dans une démarche constructive. En mars et avril 2023, des élections législatives partielles ont été organisées avec succès dans des circonscriptions électorales pour lesquelles le Conseil Constitutionnel avait invalidé les résultats en 2022. Le protocole qui a alors été mis en place a intégré la majorité des correctifs que nous avions proposés. »*

Les résultats de leurs recherches seront présentés au colloque Usenix Security cet été 2023, et ont par ailleurs été exposés en mars dernier à Tokyo au Real World Crypto Symposium qui réunissait acteurs académiques et industriels. *« Ce genre de colloque permet de créer des liens entre les deux mondes, ce qui est très important pour nous car le passage de la théorie à la pratique est pertinent pour nos recherches. Sur le papier, certaines solutions paraissent très efficaces mais leur mise en œuvre pratique n'est pas forcément aussi simple. Le but est vraiment de permettre à chacun d'avancer, que ce soient les acteurs industriels dans le domaine de la sécurité informatique ou nous, chercheurs, dans le développement d'une recherche en adéquation avec les problématiques et contraintes d'applications de la vie réelle, comme le vote électronique. »*