

L'État hors la loi : Disputatio sur la continuité juridique en cas de défaillance des infrastructures numériques

Quaestio

L'État français dispose-t-il des moyens juridiques de continuer à agir lorsque les infrastructures dont dépend son action deviennent indisponibles ?

La question est moins étroite qu'il n'y paraît. Une cyberattaque n'est qu'une manière parmi d'autres de faire disparaître, pour un temps, les instruments ordinaires de l'administration. Il peut s'agir d'une panne informatique massive, d'une rupture électrique prolongée, de la destruction physique d'un centre de données, de la défaillance d'un prestataire, d'une catastrophe naturelle, d'une guerre ou, plus prosaïquement et peut-être plus dangereusement, d'une défaillance logicielle systémique.

Dans tous ces cas, le problème n'est pas nécessairement que l'État ne sache plus ce qu'il doit faire. Il peut savoir parfaitement ce qu'il doit faire et même disposer, en droit, du pouvoir de le faire.

Le problème est plus embarrassant : comment l'État continue-t-il à produire des actes juridiques lorsque le dispositif technique qui permet normalement de les transmettre, de les authentifier, de les notifier ou d'en conserver la preuve n'est plus disponible ?

La question concerne donc moins la puissance publique que sa continuité juridique.

Videtur quod sic

Il semble d'abord que le droit français ait largement prévu l'hypothèse de la crise.

La Constitution connaît l'interruption du fonctionnement régulier des pouvoirs publics constitutionnels. L'article 16 permet au Président de la République de prendre les mesures exigées par les circonstances lorsque les institutions de la République, l'indépendance de la Nation, l'intégrité du territoire ou l'exécution des engagements internationaux sont menacées d'une manière grave et immédiate et que le fonctionnement régulier des pouvoirs publics constitutionnels est interrompu. Le texte prévoit en outre des consultations et un contrôle dans la durée.

Une catastrophe majeure, une guerre ou une attaque numérique d'une ampleur exceptionnelle pourraient donc, selon leurs effets, placer le pays dans le champ de cette disposition.

Mais il faut aussitôt écarter une facilité de raisonnement.

L'article 16 n'est pas un « mode dégradé » constitutionnel. Il ne suffit pas qu'une administration ne puisse plus accéder à ses serveurs. Il faut que les conditions très particulières du texte soient réunies, notamment l'atteinte grave et immédiate aux intérêts énumérés par la Constitution et l'interruption du fonctionnement régulier des pouvoirs publics constitutionnels. Et les mesures prises doivent avoir pour objet de donner à ces pouvoirs les moyens d'accomplir leur mission.

L'article 16 peut donc faire partie de la réponse à une crise extrême. Il n'est pas la réponse générale à une panne.

Le droit de l'état d'urgence, celui de l'état de siège, les mécanismes de réquisition et les dispositions du code de la

défense offrent eux aussi à l'État des moyens d'action considérables.

Enfin, le droit administratif connaît depuis longtemps la théorie des circonstances exceptionnelles.

De *Heyriès* à *Dames Dol et Laurent*, le Conseil d'État a admis que, dans des circonstances extraordinaires, l'administration puisse s'affranchir de certaines règles ordinaires lorsque cette dérogation est nécessaire à la continuité des services publics. Le juge ne renonce pas pour autant à tout contrôle : il vérifie notamment la réalité des circonstances, l'impossibilité d'agir régulièrement et la nécessité de la mesure.

Il serait donc faux de prétendre que le droit français ne sait rien faire lorsque la normalité disparaît.

Il sait faire beaucoup.

Il sait même, dans certaines circonstances, autoriser l'administration à faire autrement.

Sed contra

Il reste une question.

Autrement, comment ?

C'est ici que les choses se compliquent.

Les régimes de crise ont principalement été conçus pour permettre à l'autorité publique d'agir malgré une perturbation grave de l'ordre politique, militaire, social ou matériel.

Ils disent assez bien **quels pouvoirs supplémentaires l'État peut exercer.**

Ils disent beaucoup moins clairement **dans quelles formes juridiques l'administration peut continuer à exercer ses**

pouvoirs lorsque les infrastructures ordinaires de ces formes ont disparu.

Un état d'urgence peut permettre une mesure de police.

Une réquisition peut permettre de mobiliser une ressource.

La cyberdéfense peut permettre de neutraliser une attaque.

Les circonstances exceptionnelles peuvent, sous le contrôle du juge, justifier une dérogation à certaines règles.

Mais aucun de ces mécanismes ne constitue, à lui seul, un droit général du mode dégradé.

Il ne s'agit pas d'un détail.

Un préfet peut conserver toute sa compétence et être néanmoins privé du système qui permet normalement de transmettre un acte.

Une collectivité peut savoir exactement quelle décision elle veut prendre et ne plus disposer du dispositif technique qui assure sa télétransmission.

Une administration peut avoir le pouvoir de payer et ne plus pouvoir ordonner le paiement par le système qui l'exécute.

Un service peut avoir à notifier une décision urgente alors que son système de messagerie, d'identité numérique ou de signature est indisponible.

Le pouvoir subsiste.

La forme par laquelle il s'exerce manque.

Un état d'exception ne résout pas nécessairement cette difficulté.

Il ne rallume pas un annuaire.

Respondeo

Il faut donc distinguer deux problèmes.

Le premier est celui du **pouvoir d'agir**.

Le second est celui de la **continuité des conditions juridiques de l'action**.

Sur le premier terrain, l'État français est loin d'être démuní.

Sur le second, la situation est moins nette.

Cette distinction mérite d'être formulée avec précaution. Il serait excessif de soutenir qu'une panne informatique rendrait par elle-même les actes administratifs nuls. Il serait tout aussi excessif d'affirmer que le papier cesserait partout de produire un quelconque effet juridique.

Le problème est plus précis.

La dématérialisation a progressivement fait du support numérique, dans certaines procédures, une composante de la procédure elle-même.

Le code des relations entre le public et l'administration en fournit un exemple clair. Lorsqu'une administration met en place un téléservice réservé à l'accomplissement de certaines démarches, elle peut imposer son utilisation pour que la saisine électronique soit régulière. Le même code organise d'ailleurs de manière générale les échanges électroniques entre l'administration et le public.

Ce dispositif est parfaitement rationnel en temps normal.

Il devient juridiquement intéressant lorsque le téléservice cesse de fonctionner.

Que devient alors la démarche qui devait obligatoirement

passer par lui ?

La réponse n'est pas nécessairement « rien ». Il peut exister une autre voie prévue par le texte particulier, une procédure de secours, une possibilité de dépôt physique, une règle spéciale ou, dans certains cas, le recours ultérieur à la théorie des circonstances exceptionnelles.

Mais précisément : **la réponse dépend alors de la procédure considérée, de la nature de l'indisponibilité et de la règle applicable.**

Il n'existe pas, de manière générale, un principe simple que pourrait appliquer n'importe quel agent :

le système est indisponible ; voici le régime juridique qui s'applique désormais.

C'est cette absence de règle transversale que la dématérialisation rend progressivement plus visible.

La même évolution apparaît dans la chaîne financière publique.

La généralisation en cours de la facturation électronique ne constitue pas seulement une réforme comptable. Elle organise progressivement les échanges de factures autour de plateformes et de procédures électroniques déterminées. Pour les fournisseurs de l'État et des collectivités, cette évolution s'inscrit dans un environnement déjà largement dématérialisé, notamment autour de Chorus Pro.

Là encore, le problème n'est pas de savoir si une facture peut, en théorie, être imprimée sur une feuille de papier. La question est de savoir ce qui advient de la procédure lorsqu'un système dont dépend sa transmission, sa réception ou son traitement devient indisponible.

Une panne de quelques heures n'a évidemment pas les mêmes conséquences qu'une indisponibilité prolongée. Et toutes les

défaillances ne justifieraient pas un régime dérogatoire. Mais si une infrastructure critique cesse durablement de fonctionner, la question devient inévitable : les délais continuent-ils à courir ? Selon quelles modalités le fournisseur peut-il être réputé avoir transmis sa facture ? Comment l'administration établit-elle la date de réception ? Comment garantit-on la continuité du paiement ?

Il ne s'agit pas de prétendre qu'une panne de plateforme rendrait les créances inexistantes ou les paiements juridiquement impossibles. Il s'agit de constater qu'à mesure que la procédure devient électronique, la continuité de l'infrastructure qui la porte devient elle-même une condition pratique de la continuité financière de l'État.

Non pas le numérique : la dépendance

Il faut alors élargir le problème.

La cyberattaque est un cas spectaculaire parce qu'elle donne à la panne un adversaire identifiable.

Mais juridiquement, la cause de l'indisponibilité importe parfois moins que son effet.

Une même administration peut se trouver dans la même situation si son système tombe à la suite :

- d'une panne informatique massive ;
- d'une cyberattaque ;
- d'une rupture électrique prolongée ;
- de la destruction physique d'un centre de données ;
- de la défaillance d'un prestataire informatique ou d'un opérateur essentiel ;
- d'une catastrophe naturelle ;
- d'une guerre ;
- ou d'une défaillance logicielle systémique affectant

simultanément des systèmes que l'on croyait indépendants.

Dans le premier cas, le serveur est peut-être intact mais inaccessible.

Dans le deuxième, il est attaqué.

Dans le troisième, il n'est plus alimenté.

Dans le quatrième, il a disparu.

Dans le cinquième, le prestataire qui l'exploite ne peut plus assurer le service.

Dans le sixième, le bâtiment est détruit.

Dans le septième, l'infrastructure est physiquement ou militairement compromise.

Dans le dernier, le système fonctionne peut-être parfaitement : c'est précisément son fonctionnement normal qui produit une erreur.

Pour le juriste, ces situations ne sont évidemment pas identiques.

Leurs régimes de responsabilité, leurs causes et les pouvoirs qu'elles déclenchent peuvent être très différents.

Mais elles ont un point commun : **l'administration peut perdre l'accès à l'infrastructure dont dépend une formalité juridique sans avoir perdu sa compétence pour accomplir l'acte.**

C'est cette situation commune qu'il faudrait prendre pour objet.

Ad primum : les circonstances

exceptionnelles ne suffisent-elles pas ?

C'est la première objection, et la plus sérieuse.

On pourrait soutenir que le droit a déjà la souplesse nécessaire.

Heyriès en fournit précisément l'exemple. Le Conseil d'État admet que, dans une situation exceptionnelle, l'administration puisse déroger aux règles ordinaires lorsque cela est nécessaire à la continuité des services publics. Le juge vérifie notamment que l'administration était effectivement dans l'impossibilité d'agir régulièrement.

Pourquoi créer autre chose ?

La réponse n'est pas que la théorie serait inutile.

Elle est qu'elle ne remplit pas exactement la même fonction.

La théorie des circonstances exceptionnelles est principalement une **doctrine de justification et de contrôle**. Elle permet au juge, lorsque le litige survient, d'apprécier si l'administration pouvait légalement agir comme elle l'a fait.

Ce que l'on pourrait ajouter serait une **règle de conduite préalable**.

À trois heures du matin, l'agent confronté à une indisponibilité massive ne devrait pas avoir à se demander quelle indulgence le juge manifestera dans deux ans.

Il devrait pouvoir savoir :

- qui constate l'indisponibilité ;
- à partir de quel seuil le mode dégradé est déclenché ;
- quelles formalités peuvent être accomplies autrement ;

- comment identifier l'auteur de l'acte ;
- comment en établir la date ;
- comment en conserver la preuve ;
- quand la régularisation est nécessaire ;
- et quelles conséquences entraîne l'impossibilité de régulariser.

La différence est donc moins entre **exception** et **normalité** qu'entre **dérogation improvisée** et **dérogation pré-organisée**.

Ce n'est pas la même chose.

Et cette organisation préalable serait précisément conforme à l'esprit même de l'État de droit : ce n'est pas parce que les circonstances sont exceptionnelles que les règles doivent disparaître ; c'est une raison supplémentaire pour que les règles applicables à l'exception soient connues avant l'exception.

Ad secundum : l'article 16 ne permet-il pas déjà de tout faire ?

L'objection est séduisante, mais elle confond l'ampleur du pouvoir avec son objet.

L'article 16 est conçu pour une situation dans laquelle les intérêts fondamentaux de la Nation sont gravement et immédiatement menacés et où le fonctionnement régulier des pouvoirs publics constitutionnels est interrompu. Ses mesures doivent permettre à ces pouvoirs de retrouver les moyens d'accomplir leur mission.

Il peut donc constituer un instrument de sauvegarde dans une crise systémique.

Mais il n'est pas nécessairement pertinent pour une situation plus étroite : un système administratif majeur indisponible pendant plusieurs heures ou plusieurs jours, alors que les

institutions constitutionnelles continuent à fonctionner.

Il serait étrange de devoir recourir à l'article 16 pour savoir si une décision administrative peut exceptionnellement être signée sur papier parce que l'infrastructure de signature électronique est hors service.

L'article 16 est une réponse à une crise constitutionnelle.

Le problème posé ici peut apparaître bien avant.

Ad tertium : la continuité administrative est-elle déjà garantie par les plans de continuité ?

Elle l'est, en partie.

Les administrations, les opérateurs et les infrastructures critiques disposent de dispositifs de continuité, de sauvegarde, de redondance et de reprise d'activité. Il serait donc faux de raisonner comme si une panne d'un serveur équivalait immédiatement à une disparition de l'État numérique.

Mais cette objection déplace plutôt qu'elle ne supprime le problème.

Un plan de continuité peut prévoir qu'un système A soit remplacé par un système B.

Il peut prévoir un site de secours, des sauvegardes, des moyens de communication alternatifs ou une alimentation électrique autonome.

Tout cela est indispensable.

Mais supposons que A et B soient indisponibles.

Ou que le site de secours fonctionne techniquement sans que les agents disposent des moyens d'authentification nécessaires.

Ou que la sauvegarde soit intacte mais que l'application permettant de l'exploiter soit affectée.

Ou qu'un prestataire essentiel soit lui-même indisponible.

Ou que la panne ne soit pas matérielle mais logique et touche simultanément plusieurs environnements réputés indépendants.

Le plan de continuité répond alors à une question opérationnelle :

comment reprendre le service ?

Il reste une question juridique :

que peut-on valablement faire pendant que le service n'est pas repris ?

Les deux questions doivent être traitées ensemble.

Ad quartum : le problème n'est-il pas seulement celui de la preuve ?

L'objection est également fondée.

Une panne ne rend pas nécessairement un acte inexistant ou nul. Elle peut surtout rendre plus difficile la preuve de son auteur, de sa date, de sa transmission ou de sa réception.

Il faut donc éviter de confondre quatre notions :

l'existence de l'acte, sa validité, son opposabilité et sa preuve.

Elles ne se confondent pas.

C'est précisément pourquoi un régime du mode dégradé devrait s'attacher moins à proclamer que « le papier vaut numérique » qu'à organiser la chaîne de confiance.

Qui a décidé ?

À quelle heure ?

Avec quelle compétence ?

Sur quel fondement ?

Quel destinataire a reçu la décision ?

Quel document permet de le démontrer ?

Que devient cette preuve lorsque les systèmes sont restaurés ?

Le véritable sujet est donc peut-être moins une prétendue « nullité numérique » que la **continuité des conditions juridiques d'authentification et de preuve de l'action administrative**.

Cette formulation est moins spectaculaire.

Elle est aussi plus exacte.

Ad quintum : une solution n'existe-t-elle pas déjà, administration par administration ?

Souvent, oui.

Certaines procédures connaissent leurs propres mécanismes de secours. Certaines administrations ont des dispositifs papier. Certaines infrastructures sont redondées. Certaines décisions peuvent être prises autrement.

Il ne faut donc pas inventer une lacune générale là où

existent de nombreuses solutions particulières.

Mais cette dispersion constitue précisément une difficulté.

La résilience d'un État ne devrait pas dépendre uniquement de la question de savoir si chaque administration a, de son côté, prévu une procédure de secours suffisamment complète.

Plus les administrations sont interdépendantes, plus la continuité devient une question d'architecture générale.

Un système peut être techniquement redondant et juridiquement fragile.

Un autre peut être juridiquement souple et techniquement vulnérable.

La résilience véritable se situe dans l'intersection des deux.

Ad sextum : et si la cause de la panne était une guerre ?

La guerre rend la question plus évidente, mais non différente dans son principe.

Le droit des conflits armés, les pouvoirs de défense nationale et les régimes constitutionnels de crise peuvent alors entrer en jeu. La jurisprudence des circonstances exceptionnelles est elle-même née dans un contexte de guerre. Le Conseil d'État rappelle d'ailleurs que cette théorie n'a jamais signifié une disparition pure et simple du contrôle juridictionnel : même en période de guerre, les garanties fondamentales de l'État de droit ne sont pas simplement abolies.

La guerre ne constitue donc pas un argument pour renoncer à la légalité.

Elle constitue plutôt l'un des meilleurs arguments pour préparer à l'avance les formes juridiques de la continuité.

Car la guerre n'est pas le seul événement capable de rendre indisponible une infrastructure.

Et si une règle n'est conçue que pour la guerre, elle risque de ne rien offrir lorsque le même effet survient un mardi matin, sans ennemi identifiable, à la suite d'une panne logicielle.

Ad septimum : faut-il alors un « état d'urgence numérique » ?

Non.

Ce serait probablement la mauvaise réponse.

La création d'un nouveau régime d'exception donnerait à la crise numérique une place institutionnelle qui n'est pas nécessairement justifiée et risquerait surtout de confondre deux problèmes : **la capacité de l'État à faire face à la menace et sa capacité à continuer à produire des actes juridiques lorsque ses infrastructures sont indisponibles.**

Le second problème appelle moins de pouvoirs que de prévisibilité.

Il ne s'agit pas d'autoriser l'administration à faire n'importe quoi parce que les ordinateurs sont en panne.

Il s'agit de déterminer à l'avance ce qu'elle peut faire précisément parce que les ordinateurs sont en panne.

Respondeo iterum : un droit du mode dégradé

Ce droit pourrait être relativement modeste.

Il ne nécessiterait pas nécessairement une nouvelle théorie générale des circonstances exceptionnelles.

Il pourrait prendre la forme d'un régime transversal de continuité juridique applicable à l'indisponibilité grave d'une infrastructure nécessaire à l'accomplissement d'une formalité.

Le déclenchement pourrait être subordonné à une constatation formelle de l'indisponibilité, par l'autorité compétente ou selon une procédure définie à l'avance.

À compter de cette constatation, certaines formalités dématérialisées obligatoires pourraient temporairement être accomplies par des moyens substitutifs expressément déterminés.

Mais l'équivalence devrait être encadrée.

Il faudrait prévoir :

La constatation. Qui peut déclarer l'indisponibilité et selon quels critères ?

Le périmètre. Quelles procédures sont affectées ? Toutes ne le seront pas nécessairement.

L'équivalence. Quel support ou quel moyen de substitution produit les mêmes effets ?

L'authentification. Comment établir l'identité et la compétence de l'auteur lorsque le système d'identité est lui-même indisponible ?

La datation. Comment établir qu'un acte a été pris avant, pendant ou après la période de dégradation ?

La preuve. Quel registre, document ou témoignage permet d'en conserver une trace fiable ?

La régularisation. Dans quel délai le document ou l'information doit-il être réintroduit dans le système une fois celui-ci restauré ?

Le contentieux. Quel régime s'applique lorsqu'une régularisation n'a pas été possible ou lorsqu'un destinataire conteste l'authenticité de l'acte ?

La durée. Le mode dégradé doit être temporaire, contrôlé et réévalué.

Cette dernière exigence est essentielle.

Le mode dégradé ne doit pas devenir une nouvelle normalité administrative par la simple inertie.

Une réquisition adaptée

Le second chantier est celui des ressources nécessaires à la reprise.

Une crise numérique ne nécessite pas seulement des locaux ou des véhicules. Elle peut nécessiter des compétences rares, des capacités de calcul, des équipements de télécommunication, des capacités d'hébergement, des moyens de restauration des données ou l'intervention d'équipes privées spécialisées.

Le droit des réquisitions fournit déjà une partie de cette architecture.

Mais la question mériterait d'être précisée pour les ressources numériques critiques : compétences, capacités techniques, hébergement, interconnexions, équipements et services indispensables à la restauration d'une fonction publique.

Il ne s'agit pas davantage ici d'accroître indéfiniment les pouvoirs de l'administration.

Il s'agit de faire correspondre les moyens juridiques de la réquisition à la nature contemporaine des ressources dont dépend la continuité de l'État.

Une continuité au-delà des frontières

Reste la donnée.

La résilience suppose parfois qu'une infrastructure puisse survivre ailleurs qu'à l'endroit où elle est habituellement exploitée.

L'Estonie offre à cet égard un exemple intéressant, mais qu'il faut présenter exactement.

L'accord conclu avec le Luxembourg en 2017 ne confère pas aux serveurs estoniens un vague « statut diplomatique ». Il prévoit quelque chose de plus précis : les équipements et licences concernés sont considérés comme des biens de l'Estonie et bénéficient d'une immunité ; les données et systèmes d'information conservés dans les locaux sont considérés comme des archives estoniennes et ces archives sont déclarées inviolables ; le Luxembourg accorde par ailleurs aux communications officielles le traitement réservé aux missions diplomatiques.

L'intérêt du modèle n'est donc pas simplement technique.

L'Estonie n'a pas seulement copié ses données.

Elle a organisé juridiquement la protection de cette copie dans un autre État.

C'est une distinction essentielle.

Une sauvegarde est une mesure informatique.

Une sauvegarde dont le statut, l'inviolabilité, les équipements et les communications sont protégés par un accord international devient un élément de la continuité juridique de l'État.

La question française pourrait être posée dans les mêmes termes, sans qu'il soit nécessaire de reproduire exactement le modèle estonien.

Certaines données régaliennes devraient-elles pouvoir être répliquées hors du territoire national sous un régime juridique prédéfini ?

La réponse n'est certainement pas uniforme. Les exigences de souveraineté, de secret, de protection des données et de sécurité nationale imposeraient des distinctions considérables.

Mais le principe mérite d'être discuté.

La souveraineté ne consiste pas toujours à empêcher une donnée de franchir une frontière.

Elle peut aussi consister à faire en sorte que, si elle la franchit pour survivre, **son statut juridique ne disparaisse pas avec elle.**

Conclusio

Il serait facile de conclure que l'État français est insuffisamment préparé à une catastrophe numérique.

Ce serait trop simple.

Il existe des dispositifs de cyberdéfense, des plans de continuité, des systèmes redondants, des régimes de crise, des mécanismes de réquisition et une jurisprudence administrative capable, dans certaines circonstances, de reconnaître la nécessité de déroger aux règles ordinaires.

Le problème est ailleurs.

Ces dispositifs répondent à des questions différentes.

La cyberdéfense cherche à empêcher ou à neutraliser l'attaque.

La redondance cherche à maintenir l'infrastructure.

Le plan de continuité cherche à reprendre le service.

Le régime de crise donne, lorsque ses conditions sont réunies, des pouvoirs supplémentaires.

La théorie des circonstances exceptionnelles permet au juge de tenir compte de l'impossibilité d'agir normalement.

Mais entre ces mécanismes subsiste une question très concrète :

que vaut juridiquement l'acte accompli pendant l'intervalle où l'infrastructure nécessaire à sa forme ordinaire est indisponible ?

Cette question peut se poser sans cyberattaque.

Elle peut naître d'une panne massive, d'une coupure électrique, de la destruction d'un data center, de la faillite ou de la défaillance d'un prestataire, d'une catastrophe naturelle, d'une guerre ou d'un défaut logiciel qui se propage simultanément à plusieurs systèmes.

Le point commun n'est pas la nature de l'événement.

C'est la dépendance.

L'État contemporain dépend d'infrastructures qui ne sont plus seulement des instruments matériels de son action. Dans certaines procédures, elles participent désormais à la manière dont le droit est produit, transmis, authentifié et conservé.

Il faut donc peut-être cesser de parler seulement de **résilience numérique**.

La question est celle de la **résilience juridique d'un État numérisé**.

Elle suppose de prévoir non seulement comment restaurer les

serveurs, mais comment continuer à produire des actes valables, opposables et prouvables pendant leur indisponibilité.

Il ne s'agit pas de créer un pouvoir d'exception supplémentaire.

Il s'agit de faire quelque chose de beaucoup moins spectaculaire : écrire à l'avance les règles de la panne.

Déterminer qui constate.

Déterminer ce qui peut être fait.

Déterminer comment.

Déterminer comment le prouver.

Déterminer comment revenir à la normale.

La véritable souveraineté numérique ne réside peut-être pas seulement dans la possession des infrastructures, ni même dans leur invulnérabilité – qui n'existe pas.

Elle réside aussi dans la capacité de l'État à demeurer juridiquement intelligible lorsque ces infrastructures cessent de fonctionner.

Nous avons prévu comment gouverner dans l'exception.

Il reste à prévoir comment le droit continue de fonctionner lorsque l'outil qui le porte ne fonctionne plus.

Rendez-vous le vendredi 18

septembre, Palais du Grand Large, à
Saint-Malo à l'occasion du 4e
colloque national de Souveraine
Tech : « Résilience des
Infrastructures et Technologies
Critiques »

4^E COLLOQUE DE SOUVERAINE TECH

RÉSILIENŒ DES INFRASTRUCTURES ET TECHNOLOGIES CRITIQUES

18/09/2026 - SAINT-MALO
PALAIS DU GRAND LARGE