



# TRIP D'AUTOMNE 2024

26 et 27 novembre

Intervention de Clara CHAPPAZ

---

## INTERVENTION DE CLARA CHAPPAZ

**SECRETAIRE D'ÉTAT AUPRES DU MINISTRE DE L'ENSEIGNEMENT SUPERIEUR ET DE LA RECHERCHE, CHARGÉE DE L'INTELLIGENCE ARTIFICIELLE ET DU NUMÉRIQUE**

Intervenants :

■ **Patrick CHAIZE**  
Président de l'Avicca

■ **Clara CHAPPAZ**  
Secrétaire d'État chargée de l'Intelligence artificielle et du Numérique

*Seul le prononcé fait foi*

### Patrick CHAIZE, Président de l'Avicca

Madame la ministre, chère Clara, merci infiniment de votre présence. Nous sommes en effet heureux de vous accueillir pour votre premier colloque TRIP. Vous avez été la première, dès votre prise de fonction, à répondre favorablement à notre invitation, ce dont je vous remercie très sincèrement.

Il faut dire que nous travaillons sur tous vos sujets depuis quelque temps déjà, que ce soit en interne, entre membres, ou bien lors de nos colloques annuels. Outre la transposition de la Directive européenne NIS2, à laquelle nous venons de consacrer cette table ronde, nous travaillons à l'échange de bonnes pratiques entre collectivités, à la mutualisation des outils, comme à la montée en compétence des territoires. Nous contribuons depuis son

origine au groupe de travail Collectivités de Cybermalveillance.gouv.fr comme au relais des messages de l'ANSSI auprès de nos membres.

S'agissant de l'intelligence artificielle, nous avons abordé il y a un an l'IA frugale avec la présentation des lauréats du premier appel à projet démonstrateur d'IA frugale au service de la transition écologique des territoires. Nous nous étions alors également interrogés sur la place de l'IA dans nos territoires. Et puis, nous avons débattu de l'IA dans presque tous ses états, éducatifs, citoyens, cyber, au colloque TRIP de printemps 2024. Et cet après-midi, nous allons présenter à la fois des outils d'analyse d'images pour les réseaux télécoms et des exemples de formation des agents de nos collectivités aux atouts et limites des intelligences artificielles génératives (IAG).

L'IAG que nous avons déjà testée lors d'un datathon dédié, car le meilleur moyen de comprendre le potentiel de l'IA dans un contexte professionnel reste pour nous de l'expérimenter. L'équipe a même expérimenté l'IA dans la conception artistique par la composition d'une chanson que nous avons eu l'occasion d'écouter hier matin lors de notre Assemblée générale.

S'agissant des startups, autre sujet qui vous est cher, nous y sommes attentifs depuis plusieurs années, notamment au travers des expérimentations pionnières dans les territoires durables et connectés que nous appelions auparavant territoires intelligents ou smart. C'est un des sujets que nous partageons le plus avec la filière, au travers d'une étroite et durable collaboration avec InfraNum.

Un dernier petit message avant de vous passer la parole. Je pressens que je vais devoir batailler ferme avec mon collègue Damien Michelet pour sauver certains budgets menacés. Je pense de manière non exclusive à celui de l'inclusion numérique, qui nous inquiète particulièrement. Je compte, madame la ministre, sur votre soutien et celui de vos collègues du Gouvernement pour faire en sorte que les choses soient rétablies. Merci à nouveau de votre présence et je vous laisse maintenant la parole qui, soyez-en sûre, est fortement attendue sur tous les sujets techniques, juridiques et stratégiques pour tous nos territoires.

**Clara CHAPPAZ, Secrétaire d'État auprès du ministre de l'enseignement supérieur et de la recherche, chargée de l'intelligence artificielle et du numérique :**

---

Monsieur le Président de l'Avicca, cher Patrick,

Mesdames et Messieurs les Parlementaires,

Mesdames et Messieurs les élus, chères toutes,

chères tous,

je suis vraiment très heureuse de me retrouver parmi vous pour cette deuxième journée du TRIP et je suis ravie d'apprendre que je suis la première à venir ici. Ça me semblait absolument fondamental vu tous les sujets que vous traitez et qui sont extrêmement importants pour moi dans cette période. Cet événement est devenu incontournable, nous en parlions tout à l'heure, depuis 2007.

En fait, l'écosystème numérique a beaucoup changé depuis, mais vous avez avec constance porté la mutation de cet écosystème et abordé collectivement les enjeux cruciaux du développement du numérique pour nos territoires. Aujourd'hui, ces enjeux me tiennent particulièrement à cœur. Vous avez à l'instant parlé de NIS2, il me semble. La cybersécurité et la résilience, l'inclusion numérique, mais aussi l'intelligence artificielle sont des sujets cœur à mon portefeuille. Je voudrais d'abord vous féliciter toutes et tous, et vous féliciter personnellement, cher Patrick, pour la qualité de cet événement et pour votre investissement qui est reconnu sur les questions numériques depuis fort longtemps. Les enjeux dont vous discuterez aujourd'hui, en particulier celui que vous venez d'aborder ici avec NIS2, sont au cœur de cette feuille de route.

Pour prendre un peu de hauteur et vous partager quelques éléments, je suis en train en effet de me fixer quatre grandes priorités en tant que secrétaire d'État chargée de l'intelligence artificielle et du numérique.

La première, faire de la France une grande puissance de l'IA, pas simplement pour maîtriser cette technologie, mais vraiment pour la mettre au service de la société et des Français qui trop souvent se sentent un peu démunis par rapport à cette technologie.

La deuxième, soutenir notre tissu de jeunes entreprises, porteuses d'innovation et ce tout au long du cycle de leur vie.

La troisième, protéger notre espace numérique, nous en parlions à l'instant, et construire un cadre de régulation équilibrée qui favorise l'innovation tout en préservant notre souveraineté.

Et enfin, promouvoir un numérique inclusif, responsable et durable qui profite à l'ensemble de nos concitoyens.

Ces quatre objectifs constituent une réponse aux défis toujours plus nombreux que nous devons relever. Nous, la France, mais l'Europe aussi, dans le champ du numérique et plus généralement de l'innovation et de la compétitivité. Dans le contexte mondial que nous connaissons tous, de tensions géopolitiques croissantes, de concurrence économique accrue et qui ne fera que se renforcer, de résultats électoraux lourds de conséquences, y compris chez nos alliés, l'Europe doit plus que jamais être à la hauteur. Il nous faut avancer résolument afin de concilier notre autonomie stratégique, rester maître de notre destin collectif. Pour réussir ce défi, nous devons disposer de nos propres technologies et donc continuer à les soutenir. Nous devons favoriser un développement encadré de ces technologies afin de protéger nos concitoyens contre les risques inhérents à leur diffusion tout en garantissant des usages qui reflètent nos valeurs.

Au premier rang des risques qui nous préoccupent, il y a bien sûr le risque cyber. Vous venez de l'aborder, il sera au cœur de mon propos de ce matin. Je sais que la transposition de NIS2 et son application aux collectivités territoriales est au cœur de votre attention. Je suis sûre que le représentant de l'ANSSI qui était là vous a déjà apporté de nombreuses réponses utiles. Je voudrais quand même vous dire quelques mots sur la manière dont le Gouvernement envisage l'exercice de NIS2.

Vous le savez donc, la menace cyber s'est démocratisée, dans un contexte de tensions internationales accrues, et les impératifs de résilience des infrastructures essentielles à la vie de la nation deviennent des enjeux existentiels. Qu'elles soient d'origine étatique, le fait de groupes cybercriminels, liés à des tentatives d'espionnage, elles ciblent l'ensemble de notre tissu économique et administratif, de manière systémique. Toutes les organisations sont concernées, avec notamment une hausse de 30% des attaques par rançongiciels depuis 2022, qui concerne majoritairement les TPE, les PME, les collectivités territoriales et les entreprises stratégiques. Entre janvier 2022 et juin 2023, l'ANSI a traité en moyenne 10 attaques par mois contre une collectivité. Sur cette période,



la moitié des départements et 12 régions ont été touchées. Il nous faut prendre collectivement la mesure de ce chiffre. C'est une réalité très concrète, puisque nous pouvons citer en Bretagne, où j'étais la semaine dernière, la mairie de Guingamp, de Morlaix ou de Betton. Mais également cette année, la ville d'Albi, celle de Saint-Nazaire, qui a dû repasser au papier et au crayon afin d'assurer la continuité du service public. Et enfin, dans le département de l'Ain, cher au rapporteur il me semble, je peux citer la mairie d'Oyonnax début octobre, ou encore le centre hospitalier de Bourg-en-Bresse.

Le secteur de la santé n'est en effet pas en reste. L'ANSSI indique dans son rapport du 7 novembre que la part des incidents concernant le secteur de la santé a été multipliée par 4 entre 2020 et 2023. Les conséquences de ces attaques, qui sont désormais la norme, peuvent être majeures à l'échelle d'un territoire ou d'une collectivité et affecter de nombreux citoyens. Imaginons les responsables d'établissements de santé quand ils n'ont plus accès aux données de leurs patients, qui arrivent dans ces mêmes établissements et qu'il faut soigner. Il faut aussi penser aux implications d'un incident par rançongiciel contre un Département qui ne serait plus en mesure de verser les contributions sociales, ou le traitement des agents publics, ou encore le traitement des déchets pendant plusieurs semaines.

Face à ce constat d'une massification de la menace cyber, la directive NIS2 a été pensée pour nous faire entrer dans l'ère de la cybersécurité de masse. Vous le savez, ce texte implique en effet une augmentation importante du nombre d'entités régulées, de 500 à 15 000 entités. Une augmentation du nombre de secteurs régulés, de 6 à 18. Cette directive élargit également le périmètre des systèmes d'information à sécuriser, et s'applique par défaut à l'ensemble des systèmes d'information de l'entité, bien que certaines exemptions soient permises. Elle consacre, et c'est un point important, un principe de proportionnalité en prévoyant deux niveaux d'entités régulées, qui sont classées selon leur degré de criticité, leur taille et pour les entreprises, leur chiffre d'affaires.

Vous le savez aussi, la directive prévoit elle-même son application aux Régions en tant qu'entité essentielle. Mais la France a défendu lors des négociations européennes la possibilité d'appliquer ces règles aux autres niveaux de collectivité. Il s'agit d'une position nécessaire, face au constat que je viens de faire, de la multiplication des attaques qui affectent les services publics locaux, témoins de leur sécurisation insuffisante. C'est pour

cette raison, et la raison pour laquelle, le projet de loi Résilience que j'ai présenté en Conseil des ministres le 15 octobre intègre les collectivités dans ces nouvelles exigences de cybersécurité.

Pour autant, le Gouvernement et l'ANSSI n'ont pas décidé seuls en chambre de ces nouvelles exigences. Il s'agit d'un texte coconstruit avec vous, les collectivités, par l'intermédiaire des associations d'élus notamment, qui prend en compte leurs préoccupations. L'ANSSI a mené 70 consultations depuis septembre 2023 qui se poursuivent jusqu'à aujourd'hui. Elles continueront bien sûr tout au long du texte, y compris sur son volet réglementaire et pendant sa mise en œuvre. Et je compte sur vous, toutes et tous, pour nous alerter des points de préoccupation que vous auriez. J'ai moi-même eu l'occasion de m'entretenir dès ma prise de fonction avec des parlementaires, des associations d'élus, des élus eux-mêmes, des entreprises, des fédérations, à Marseille, à Rennes ou à Grenoble dans les dernières semaines. Ce dialogue est bien entendu amené à se poursuivre car c'est la seule manière pour nous et pour moi d'avoir les retours terrain qui me semblent importants dans la mise en application du texte. De ces échanges, je retiens que la directive qui est certes très ambitieuse, a suscité des interrogations de la part des entreprises et des collectivités, mais que la prise de conscience du passage à l'échelle qu'elle provoquera nous permet d'accompagner mieux les entités dans les efforts qu'elles devront fournir.

Je me réjouis d'avoir constaté que ni le principe ni les objectifs du texte ne sont remis en cause. Je pense que beaucoup d'entre vous, et certainement certains d'entre vous dans cette pièce, ont eu à faire face à un certain nombre d'incidents et de cyberattaques et que les interlocuteurs, tous les interlocuteurs avec qui j'ai pu échanger, sont pleinement convaincus de la nécessité de renforcer notre sécurité. J'ai reçu aussi des échos très positifs des nombreux acteurs et en particulier de certaines associations et de collectivités sur la méthode que l'ANSSI a employée et le dialogue qu'elle a su entretenir. Et c'est pourquoi je tiens aussi à l'en féliciter devant vous. Merci pour tout ce travail qui a été fait jusqu'ici sur ce texte. Cette méthode est la bonne, une approche proportionnée, progressive, adaptée aux moyens et à la maturité des acteurs. Elle est pleinement conforme à l'ambition du gouvernement, qui a fait de la simplification un enjeu majeur pour permettre à nos entreprises, à nos services publics, de mieux fonctionner.

Vous pouvez donc compter sur toute ma vigilance pour que ce texte limite tout risque de surtransposition tout en assurant un vrai niveau de protection. Nous devons faire de la mise en œuvre de NIS2 un exercice opérationnel, utile et pragmatique qui tienne compte des spécificités de chaque entité afin d'élever notre niveau de cybersécurité et de résilience collective de façon adaptée, proportionnée, raisonnable, mais en restant ambitieuse, car le niveau de menace est élevé.

Avec ce texte, la cybersécurité ne doit plus être perçue comme une contrainte, mais comme une opportunité. Une opportunité de mieux sécuriser les actifs essentiels à nos activités économiques et sociales. Il y aura bien sûr un travail de pédagogie, un accompagnement de l'État, en particulier de l'ANSSI, dont l'objectif premier n'est pas de sanctionner, mais bien de permettre à chacun de progresser et de se saisir des enjeux, et pleinement de ces enjeux. Enfin, l'ANSI est en train de procéder à une adaptation d'ampleur, tant en termes d'organisation que de développement de son offre de services, pour pouvoir faire passer à l'échelle son dispositif d'accompagnement.

Le Gouvernement a aussi anticipé. Grâce au programme d'accompagnement du plan de relance que j'ai cité, nous pouvons compter sur les différents acteurs, sur les réseaux territoriaux, qu'il s'agisse du GIP Acyma, des CCI, du dispositif France NUM, des campus cyber dont vous parliez à l'instant ou encore des CCIRT qui sont amenés à monter en puissance.

Dans le prolongement des mesures de simplification réglementaire en cyber que le projet de loi Résilience prévoit, la DGE et l'ANSSI travaillent pour standardiser les programmes d'aide et de conseil cyber. Ce modèle standard sera défini autour du référentiel de mesures de sécurité sur lequel les programmes existants au futur pourront s'aligner. Il nous permettra de mieux coordonner, structurer, renforcer les réseaux d'accompagnement dans tous les territoires qui sont autant d'interlocuteurs de proximité qui, je sais, vous seront utiles, et utiles à toutes les entités régulées. Ce travail s'inscrit dans la durée, au plus proche des besoins, mais produira des résultats dès la mise en œuvre du texte. Je serai particulièrement vigilante à ce que ces travaux permettent de répondre aux besoins d'accompagnement des collectivités.

L'enjeu étant bien d'aider toutes les entités concernées à monter en compétence et non pas que ce texte soit vécu comme une punition collective. La mise en conformité

s'appréciera dans la durée et vous pourrez compter sur mon soutien, sur celui de l'ANSSI, pour faire preuve de pédagogie dans son rôle de superviseur. Nous ne relâchons pas les efforts et nous devons continuer à maintenir un très haut niveau d'ambition pour protéger nos concitoyens, nos administrations et nos entreprises contre ces risques cyber qui ne font qu'augmenter. Toutefois, je me permets de vous alerter, la force d'une chaîne dépend de son maillon le plus faible. Nous ne pourrions donc atteindre notre meilleur niveau que si chacun d'entre nous place la cybersécurité au cœur de ses préoccupations et continue à se préparer aux défis qui nous attendent. Ils sont immenses.

Ce constat que je dresse sur la cybersécurité, je peux l'étendre à l'ensemble du numérique. Nous ne parviendrons pas à construire une société numérique innovante et de confiance sans que chacun de nos concitoyens puisse se reconnaître dans les mutations sociétales induites par les nouvelles technologies. Je me permets donc de vous dire quelques mots sur ce point et de reboucler avec le thème qui a été mentionné dans la table ronde précédente, puisque je sais l'inclusion numérique au cœur des échanges que vous tiendrez dans quelques instants et que ce sujet m'est particulièrement cher.

Nous estimons que 46% des Français ont confiance dans le numérique. Alors il y a deux façons de le voir. C'est un chiffre en hausse, c'est encourageant, mais c'est bien trop loin des objectifs qui nous permettront de nous engager sereinement dans la transition numérique. Et bien trop loin de mes propres objectifs pour faire des outils numériques des outils de confiance.

Comment inviter les Français à adopter les bons gestes en matière de cybersécurité s'ils ne comprennent pas ou peu les outils qu'ils ont entre les mains ? Comment faire quand une personne non diplômée sur deux estime que le numérique complique son quotidien ? Nous faisons tout pour que la confiance des Français puisse s'appuyer sur un encadrement adapté des usages numériques. Mais cette confiance ne pourra pleinement s'établir tant que nous dénombrerons 13 millions de Français qui souffrent encore d'illectronisme. Ni tant que nous accuserons un retard de plus de 25% sur l'objectif européen de 80% de populations maîtrisant les compétences numériques. Je ne vous l'apprends pas, un sentiment de déclassement s'ancre déjà chez certains de nos concitoyens. Il ne pourra qu'être renforcé par la dématérialisation grandissante des démarches administratives et par l'arrivée bien sûr de l'intelligence artificielle.

L'exclusion numérique se relève donc comme un enjeu politique majeur. Si nous ne mobilisons pas tous les moyens pour en traiter les causes, elle nous mènera directement vers un renforcement de la fracture territoriale. Être à la pointe du numérique signifie donc aussi engager l'ensemble des Français dans ce projet. Pour cela, il nous faudra premièrement répondre aux urgences et apporter une assistance aux usagers qui se sentent seuls face aux démarches administratives numérisées. Les conseillers, les aidants numériques et professionnels de l'accueil aux usagers constituent à ce titre un maillon-clé du projet de société numérique que nous souhaitons mener à son terme. Je tiens à saluer l'implication des collectivités territoriales, des associations, qui jouent un rôle crucial pour faire vivre cette politique d'inclusion numérique sur le territoire.

Deuxièmement, nous devons permettre à chacun d'acquérir une forme d'autonomie numérique, et ce, bien que les Français ne formulent pas toujours ce besoin de développer leurs propres compétences en la matière. Sur ce point, le déploiement des 4 000 conseillers numériques que vous venez de mentionner et qui a permis d'accompagner plus de 4 millions de Français depuis 2021 est un dispositif qui a fait ses preuves et je tiens à le réaffirmer devant vous. Je sais que sa trajectoire de financement est source de questionnements et le débat parlementaire permettra sans doute de faire vivre les discussions à ce sujet. Permettez-moi tout de même dès à présent de réaffirmer mon attachement à la pérennité d'une politique d'inclusion numérique ancrée dans les territoires, au plus proche de nos concitoyens.

Enfin, nous devons œuvrer pour que chacun devienne lui-même acteur du numérique, se prépare aux nouveaux métiers et potentiellement entreprenne des initiatives s'appuyant sur les nouvelles technologies. C'est le sens de l'action que j'ai entamée avec mon ministre de tutelle, Patrick HETZEL, pour renforcer la formation au numérique. C'est également le sens du dispositif Café IA, dont certains dans la salle ont peut-être entendu parler déjà, que je souhaite voir se déployer sur l'ensemble du territoire, sensibiliser les Français et les Françaises à l'intelligence artificielle, c'est notre devoir commun. Sur ce point également, le déploiement du plan France très haut débit, qui vise à garantir une couverture Internet de qualité sur l'ensemble du territoire, est un point clé sur lequel je sais mon collègue Marc FERRACCI très mobilisé. Il vous en dira probablement quelques mots.

C'est donc en impliquant chaque maillon de la chaîne, entreprises de toute taille, États, collectivités, administrations, citoyens, que nous parviendrons à bâtir une société capable d'affronter les défis contemporains liés au numérique. C'est tout le sens de la démarche que je viens d'évoquer et de ce projet de loi que je porte et qui nous aidera à renforcer la cyber-résilience de la nation. Je compte sur vous et vous pouvez compter sur moi.

Je vous remercie.

