

Guy Duplaquet : “Le réseau interministériel de l’État a permis de faciliter la transformation de l’État”

Emile Marzolf

Pourquoi le Réseau interministériel (RIE) a-t-il été créé ? Comment était construit, ou plutôt étaient construits les réseaux informatiques de l’État avant le RIE ?

Avant la mise en place du RIE, en 2013, une trentaine de réseaux ministériels plus ou moins internalisés coexistaient avec un réseau intranet qui s’appelait AdER, créé en 2000. Ce même réseau était, lui, plus ou moins interconnecté au niveau européen avec le réseau Testa. La réalité était que ces réseaux ministériels communiquaient mal entre eux et freinaient les échanges mais aussi la transformation de l’État, et pas seulement sa transformation numérique. Avec un réseau unique, l’objectif était donc d’outiller les échanges d’informations entre des services et entre applications métiers, par exemple entre les services d’enquêtes de la police et la gendarmerie et les magistrats instructeurs et le parquet, ou bien encore entre les policiers et gendarmes chargés du contrôle routier des véhicules transportant des animaux vivants et le ministère de l’Agriculture. Le RIE poursuivait aussi un objectif d’économies par la mutualisation, dans la mesure où les grands ministères bénéficiaient d’une massification de leurs achats et donc de tarifs intéressants, quand les petits ministères devaient payer beaucoup plus cher pour le même service en raison de volumes plus faibles.

Le réseau interministériel s’appuie pourtant sur des opérateurs de télécommunications privés ?

Historiquement, certains réseaux ministériels étaient très internalisés, comme au ministère de l’Intérieur, qui possédait ses équipements et louait uniquement des liaisons spécialisées à des opérateurs commerciaux. D’autres avaient des réseaux très externalisés, comme à la Justice, à l’Écologie ou à l’Agriculture, probablement pour des raisons liées à leur historique et à leur culture. La différence était néanmoins flagrante, entre un ministère de l’Intérieur doté d’un très beau réseau, mais dont le fonctionnement nécessitait des équipes considérables – plus d’une centaine d’agents – quand la Justice ne mobilisait que 3 agents sur son propre réseau, pour environ 3 000 sites utilisateurs. Chaque organisation, internalisée ou externalisée, a ses avantages et inconvénients et c’est pourquoi l’État a cherché, à travers le RIE, à construire à un réseau hybride qui convienne à tous les ministères, avec certains composants très internalisés pour offrir un très haut niveau de maîtrise, comme son épine dorsale [*le cœur du réseau, avec une capacité maximale de transmission d’informations, ndlr*] ou l’équipement de sécurité vis-à-vis d’Internet, et d’autres parties du réseau où l’on a cherché davantage de souplesse et donc d’externalisation. Typiquement, ce n’est pas le rôle de l’État de construire et déployer des liens en cuivre ou en fibre optique d’un bout à l’autre de la France, y compris en dehors de l’Hexagone. Nous avons cherché

non pas créer à une chimère, mais plutôt un réseau qui tire le meilleur des possibilités que nous offrait le code des marchés publics et les attentes de nos bénéficiaires. Le tout sans froisser les opérateurs privés, qui pouvaient être tentés de voir le RIE comme un concurrent de leurs propres réseaux. Au contraire, le RIE s'appuie sur une dizaine de ces opérateurs pour offrir la plus large couverture du territoire, mais aussi pour répondre à des besoins très différents.

L'État a cherché, à travers le RIE, à construire à un réseau hybride qui convienne à tous les ministères.

Qui sont aujourd'hui les utilisateurs du RIE ? Et qu'est-ce que sa mise en place leur a apporté ?

Près de 14 000 sites sont aujourd'hui reliés au RIE, mais cela change en réalité tous les jours. Pour environ 1 million d'utilisateurs dans la sphère État, en excluant donc ses opérateurs, les établissements publics et les collectivités. Néanmoins, nous collaborons de près avec un réseau comme Renater, le réseau de l'enseignement supérieur, sur lequel s'appuie une partie du réseau de l'État. La mise en route du RIE nous a permis de construire avant tout une culture commune et une base commune à tous les systèmes d'information de l'État, avec un modèle de sécurité et de cloisonnement généralisé à tous les services de l'État. Ce qui montre que l'État peut aussi réussir des grands projets informatiques, et qu'il faut en tirer les leçons, au même titre que des échecs. Sur le plan économique, nous avons clairement gagné avec la massification, et c'est d'autant plus vrai pour les petits ministères. Le montant est difficile à évaluer, mais les gains ont par exemple été spectaculaires pour le ministère de l'Agriculture, où je travaillais à l'époque. Si les économies générées ne se ressentent pas au niveau budgétaire, c'est parce qu'elles ont été directement reversées pour améliorer le confort des utilisateurs et le niveau de service rendu, notamment en termes de débit.

La crise du Covid a été un moment charnière pour le RIE. Comment a-t-il dû évoluer pour s'adapter à la nouvelle réalité du télétravail ?

Nous avons clairement été pris par surprise, nous aussi, avec le passage au télétravail. Mais nos équipes opérationnelles ont très vite trouvé des solutions pour assurer l'administration du réseau et sa supervision, en 24h/7, mais entièrement à distance. Nous avons dû relever des défis techniques dont chacun dans l'équipe se souviendra, notamment au niveau de l'administration technique et de l'interfonctionnement avec Internet. Notre plate-forme d'accès à Internet a été conçue pour des agents au bureau, et non en mobilité. Or, du jour au lendemain, la forme du trafic a complètement changé, au niveau du trafic entrant et sortant, ou bien encore des protocoles utilisés. On s'est soudainement retrouvés avec des VPN en masse et des flux de visioconférence en

pleine explosion, et la nécessité de configurer notre plate-forme pour absorber tout cela.

Est-ce cette même crise sanitaire qui a justifié le lancement du programme de modernisation “RIE 2.0”, en 2020, pour en améliorer la résilience, la performance et la sécurité ?

La pandémie n’a fait que légitimer le lancement de ce programme, qui aurait été lancé avec ou sans le Covid-19. En réalité, la problématique de la résilience du RIE pour assurer la continuité des services de l’État en cas de crise est apparue après son lancement, qui poursuivait d’abord un objectif de transformation et d’économies. Elle s’est ensuite imposée avec la décision d’arrêter le réseau Rimbaud et de basculer les services de téléphonie sécurisée qui y étaient acheminés. C’est ce qui a donné lieu au programme “Résilience RIE”. Plus largement, le programme RIE 2.0 vise à tirer les leçons des difficultés rencontrées ces dix dernières années, soit une génération télécom, mais aussi des points positifs, pour mieux répondre aux besoins de nos bénéficiaires. Il y a donc le volet “Résilience” pour prendre la suite du réseau Rimbaud et faire fonctionner les applications comme Osiris et Isis. Ce qui suppose de doubler l’épine dorsale pour éviter les pannes techniques. Il y a aussi le programme “RIE THD”, qui vise à assurer la bascule en fibre optique pour augmenter les débits fournis par le réseau à tous les niveaux. Nous allons par exemple rénover entièrement notre plate-forme d’accès à Internet, afin d’en booster les performances et la sécurité pour faire face à un trafic bien supérieur et surtout différent, avec davantage de flux “visio” et chiffrés. Beaucoup de ces actions sont encore à mettre en œuvre.

Je ne vais pas dire que les défenses de l’État sont impénétrables, mais nous avons su répondre à toutes les attaques diligentées contre des systèmes hébergés sur le RIE.

Mais vous réfléchissez déjà à d’autres perspectives d’évolution du RIE ?

La règle que l’on s’est fixée, c’est de coller à l’évolution des besoins de nos utilisateurs et en même temps à l’évolution du marché des services télécoms, en trouvant le bon équilibre. Pas question de répondre à des besoins trop spécifiques, sinon le risque est de se retrouver avec des solutions coûteuses et difficiles à mettre en œuvre, d’autant que que le RIE s’appuie sur de multiples opérateurs télécoms. Nous avons néanmoins déjà identifié quelques pistes de court et moyen termes. On a tous vu les images des militaires ukrainiens libérant Kherson et y déployant quasi instantanément des services de télécommunications pour les habitants grâce à SpaceX. Nous réfléchissons donc à l’utilisation de ces constellations de satellites en orbite basse, pour connecter des sites plus isolés, en particulier en outre-mer. Encore faut-il identifier une offre que l’on soit capable de maîtriser en termes de service, de sécurité et de coûts.

Un rapport d'audit du RIE [révélé par Acteurs publics en février 2022](#) pointait plusieurs faiblesses, au niveau de la sécurité, mais aussi des ressources humaines nécessaires pour faire tourner ce réseau et le faire monter en gamme. Ces difficultés sont-elles derrière vous ?

La plupart des recommandations du rapport ont été suivies. En matière de sécurité du réseau, la collaboration avec l'Anssi est excellente et nous allons déployer des outils pour exploiter les traces générées par le trafic [*afin de détecter des anomalies et des intrusions, ndlr*]. Je ne vais pas dire que les défenses de l'État sont impénétrables, mais nous avons su répondre à toutes les attaques diligentées contre des systèmes hébergés sur le RIE. Au niveau RH, nous avons conduit un travail important sur la fidélisation des agents et le *turn-over* que nous constatons est le même que pour un service opérationnel classique. Nous sommes dans la cible, avec 53 ingénieurs et techniciens dans le département.

Propos recueillis par Émile Marzolf