Décision n° 17
du 21 janvier 2015

sur l'exception d'inconstitutionnalité des dispositions de la Loi sur la cybersécurité de la Roumanie,

publiée au Moniteur officiel de la Roumanie, Partie I, n° 79 du 30 janvier 2015.

Résumé

I. Dans les motifs de l'exception d'inconstitutionnalité, les auteurs affirment que les dispositions légales sont contraires à l'article 1, paragraphes (3) et (4) relatif à l'État de droit et à l'obligation du respect de la Constitution et des lois. On estime que la loi critiquée introduit beaucoup de confusions et conditions pour les détenteurs d'infrastructures cybernétiques, qui sont susceptibles de générer des restrictions des droits et des libertés fondamentales des citoyens. Les dispositions légales ne satisfont pas aux dispositions de l'article 6 de la Loi n° 24/2000 sur les règles de technique législative pour l'élaboration des actes normatifs et violent ainsi le principe de la légalité, qui est essentiel pour le bon fonctionnement de l'État de droit.

Les auteurs de la saisine font valoir que cette loi a des problèmes fondamentaux de conception, en proposant une série de mesures à effet limitatif sur le droit prévu à l'article 26, paragraphe (1) de la Constitution relatif à la vie intime, familiale et privée, et viole manifestement les réglementations européennes en cours de discussion sur la sécurité de l'information dans le domaine numérique. En outre, la loi restreint les droits et les libertés des citoyens en octroyant l'accès à une infrastructure cybernétique et aux données fournies par celle-ci sur simple demande motivée de la part des institutions désignées par la loi, envoyée aux détenteurs des infrastructures, sans l'approbation préalable d'un juge, comme le prévoit le Code de procédure pénale ou la jurisprudence de la Cour Constitutionnelle, dans les décisions n° 440/2014 et n° 461/2014, ce qui entraîne la violation des dispositions constitutionnelles contenues à l'article 23, paragraphe (1) relatif à l'inviolabilité de la liberté individuelle et de la sécurité de la personne et à l'article 28 sur le secret de la correspondance.

D'autre part il est indiqué que les dispositions de l'article 10 de la loi désignent le Service Roumain de Renseignements comme l'autorité nationale dans le domaine de la cybersécurité, en assurant ainsi la coordination technique, l'organisation et l'exécution des activités relatives à la cybersécurité de la Roumanie. Alors que l'Union Européenne propose dans le projet de Directive NIS (Network and Information System) que les institutions responsables du domaine de la cybersécurité soient des « organismes civils, qui fonctionnent entièrement sur la base du contrôle démocratique, et ils ne devraient pas exercer des activités dans le domaine des renseignements », le législateur accorde un accès illimité et sans surveillance à l'ensemble des données informatiques détenues par des personnes de droit public et privé à des institutions qui ne remplissent aucune des conditions ci-dessus. Le fait que dans la jurisprudence récente de la Cour Constitutionnelle celle-ci a déclaré l'inconstitutionnalité de deux lois qui, en substance, violaient les mêmes droits que la loi actuellement soumise au contrôle, est une raison sérieuse pour un véritable débat des implications de la Loi de la cybersécurité et, de manière plus générale, de l'équilibre entre les droits individuels et la sécurité nationale que la Roumanie doit assurer par son système juridique. Les auteurs de la saisine allèguent que la possibilité d'accéder, sans mandat judiciaire, les données électroniques provenant de n'importe quel ordinateur, indépendamment de son propriétaire, est une ingérence injustifiée dans le droit à la protection de la correspondance, c'est-à-dire dans le droit à la vie privée, droit garanti par les articles 26 et 28 de la Constitution. Une telle ingérence n'est donc non seulement pas nécessaire dans une société démocratique, mais elle a précisément l'effet inverse : elle porte atteinte à l'essence même de la société démocratique. En effet, sous le prétexte de les protéger contre les cyberattaques, toute sorte de données peuvent être consultées à l'arbitraire du pouvoir exécutif, sans aucun contrôle de la part de la société civile.

II. En ce qui concerne ces critiques, la Cour a retenu ce qui suit :

Lors de l'examen de constitutionnalité, la Cour est partie de la prémisse que la stratégie en matière de cybersécurité et la loi sur la cybersécurité ont un rôle important à jouer pour assurer la sécurité nationale de la Roumanie, d'une part, et la protection de l'individu contre les risques pour la vie privée et la protection des données personnelles dans l'environnement en ligne, d'autre part. En ce qui concerne ces aspects analysés ensemble, par l'Arrêt du 6 septembre 1978, rendu dans l'affaire Klass et autres c. Allemagne, la Cour Européenne des Droits de l'Homme a estimé que « les sociétés démocratiques se trouvent menacées de nos jours par des formes très complexes d'espionnage et par le terrorisme, de sorte que l'État doit être capable, pour combattre efficacement

ces menaces, de surveiller en secret les éléments subversifs opérant sur son territoire » (alinéa 48). Toutefois, la Cour, consciente du risque, inhérent aux mesures de surveillance secrète, « de saper, voire de détruire, la démocratie au motif de la défendre, elle affirme qu'ils ne sauraient prendre, au nom de la lutte contre l'espionnage et le terrorisme, n'importe quelle mesure jugée par eux appropriée » (alinéa 49).

En ce qui concerne la procédure d'adoption de la loi, la Cour a constaté que, dans le cadre de la procédure législative, l'initiateur n'avait pas respecté l'obligation légale, selon laquelle le Conseil suprême de la défense nationale (CSAT) approuve les projets d'actes normatifs initiés ou émis par le Gouvernement en matière de sécurité nationale. Par conséquent, la Cour a retenu que l'acte normatif avait été adopté en violation des dispositions constitutionnelles de l'article 1, paragraphe (5), consacrant le principe de la légalité, et de l'article 119, relatives aux attributions du Conseil suprême de la défense nationale.

En procédant à l'examen du contenu normatif de la loi, la Cour a retenu qu'un élément de nouveauté apporté par celui-ci, par l'article 10, paragraphe (1), était la désignation du Service Roumain de Renseignements (SRI) en tant qu'autorité nationale en matière de cybersécurité, en assurant ainsi l'organisation et l'exécution des activités relatives à la cybersécurité de la Roumanie. À cet effet, il existe dans la structure SRI le Centre national de cybersécurité (CNSC), qui a été créé, organisé et qui fonctionne déjà dans le cadre du SRI, avec du personnel militaire spécialisé, selon des arrêts du CSAT.

En vérifiant si la réglementation du domaine concerné est conforme au droit au respect de la vie intime, familiale et privée, à l'inviolabilité du secret de la correspondance, au droit à la protection des données personnelles, valeurs fondamentales qui devraient constituer des principes directeurs de la politique de cybersécurité au niveau national, la Cour a jugé que, pour assurer un environnement d'ordre, gouverné par les principes d'un État de droit démocratique, la création ou l'identification d'un organisme chargé de la coordination des questions de sécurité des systèmes et des réseaux cybernétiques et de l'information, qui représente le point de contact pour la mise en relation avec les organismes correspondants à l'étranger, devait viser un organisme civil, qui fonctionne entièrement sur la base du contrôle démocratique, et non pas une autorité exerçant des activités dans le domaine de l'information, de l'application de la loi ou de la défense ou servant d'enceinte d'un organisme opérant dans ces domaines. L'option de désigner, en tant qu'autorité nationale en matière de cybersécurité, un organisme civil, et non pas un établissement militaire

active dans le domaine de l'information, se justifie par la nécessité d'éviter le risque de compromettre l'objectif de la loi de la cybersécurité au sens de l'utilisation des attributions octroyées par cette loi par les services de renseignements dans le but d'obtenir des informations et des données ayant pour conséquence la violation des droits constitutionnels à la vie intime, familiale et privée et au secret de la correspondance. Or, alors que le CNSC constitue une structure militaire, dans le cadre d'un service de renseignements, subordonnée à la direction de cette institution, donc sous un contrôle militaire-administratif direct, il apparaît évident qu'une telle entité ne remplit pas les conditions sur les garanties nécessaires au respect des droits fondamentaux sur la vie intime, familiale et privée et au secret de la correspondance. Pour ces raisons, la Cour a constaté que les dispositions de l'article 10, paragraphe (1) de la loi soumise au contrôle violait les dispositions constitutionnelles de l'article 1, paragraphes (3) et (5) sur l'État de droit et le principe de la légalité, ainsi que celles des articles 26 et 28 sur la vie intime, familiale et privée, respectivement le secret de la correspondance, compte tenu du manque des garanties nécessaires pour garantir ces droits.

La Cour a ensuite noté que les notions utilisées par la loi ne délimitaient pas de manière non équivoque la portée des règles contenues dans l'acte soumis au contrôle de constitutionnalité, de sorte qu'il ne revêtait pas un caractère précis et prévisible et, par conséquent, il était contraire à l'article 1, paragraphe (5) de la Loi fondamentale. Ainsi, la définition des termes « détenteurs d'infrastructures cybernétiques » est particulièrement importante, car l'inclusion dans cette catégorie implique pour les personnes concernées l'obligation de respecter les dispositions de la loi, d'une part, et la justification, pour les autorités désignées par la loi ayant des compétences dans le domaine de la cybersécurité, d'ordonner des mesures particulières à leur égard. En outre, la disposition en vertu de laquelle l'accès aux données personnelles détenues par les personnes qui tombent sous l'incidence de la loi se réalise sur les « données détenues, pertinentes dans le cadre de la demande » permet l'interprétation selon laquelle les autorités désignées par la loi devraient avoir accès à toutes les données stockées dans ces infrastructures cybernétiques, si les autorités estiment que les données respectives sont pertinentes. On note ainsi le caractère non-prévisible de la réglementation, tant en termes du type de données consultées, que de l'évaluation de la pertinence des données requises, de nature à créer les conditions préalables d'applications discrétionnaires par les autorités publiques. Concrètement, les données concernées aboutissent à des conclusions très précises concernant la vie privée des personnes dont les données ont été

conservées, conclusions qui peuvent porter sur les habitudes de la vie quotidienne, les lieux de séjours permanents ou temporaires, les déplacements quotidiens ou d'autres mouvements, les activités exercées et les relations sociales de ces personnes et les milieux sociaux fréquentés par elles. Or, une telle limitation de l'exercice du droit au respect de la vie intime, familiale et privée et au secret de la correspondance, ainsi que de la liberté d'expression doit être effectuée de façon claire, prévisible et dépourvue d'ambiguïté, de manière à écarter, dans la mesure du possible, l'éventualité de l'arbitraire ou de l'abus des autorités dans ce domaine.

La Cour a également constaté que la loi critiquée se limitait à indiquer les autorités pouvant demander l'accès aux données détenues sur la base d'une demande motivée, sans régir la modalité d'effectuer l'accès effectif aux données détenues, de sorte que les personnes dont les données ont été conservées disposent de garanties suffisantes pour assurer la protection contre les abus et contre tout accès ou utilisation illicites. Ainsi, la loi ne prévoit pas de critères objectifs visant à limiter au strict minimum le nombre de personnes qui ont accès et peuvent ensuite utiliser les données conservées et n'établit pas que l'accès des autorités nationales aux données stockées est subordonné au contrôle préalable effectué par une instance judiciaire, limitant cet accès et leur utilisation à ce qui est strictement nécessaire pour atteindre l'objectif poursuivi. Les garanties légales sur l'utilisation concrète des données retenues ne sont pas suffisantes et appropriées pour éliminer la crainte que les droits personnels, d'ordre intime, sont violés, de façon à ce que leur manifestation puisse être effectuée d'une manière acceptable. Les demandes d'accès aux données retenues en vue de leur utilisation aux fins prévues par la loi, formulées par les organes d'État désignés comme autorités dans le domaine de la cybersécurité pour leurs domaines d'activité, ne font pas l'objet de l'autorisation ou de l'approbation de l'instance judiciaire, manquant ainsi la garantie d'une protection efficace des données conservées contre les risques d'abus, ainsi que contre tout accès et toute utilisation illicites de ces données. Cette circonstance est susceptible de constituer une ingérence dans les droits fondamentaux à la vie intime, familiale et privée et au secret de la correspondance et, partant, elle est contraire aux dispositions constitutionnelles qui consacrent et protègent ces droits.

Pour le suivi de son analyse, la Cour a observé que la modalité d'établir les critères pour sélectionner les infrastructures cybernétiques d'intérêt national et, partant, les détenteurs d'infrastructures cybernétiques d'intérêt national (ICIN) ne satisfaisait pas aux exigences de prévisibilité, sécurité juridique et transparence. En effet, la référence à une législation infra-légale,

respectivement aux arrêtés du Gouvernement, actes normatifs caractérisé par un degré accru d'instabilité, pour la réglementation des critères selon lesquels deviennent incidentes des obligations en matière de sécurité nationale viole le principe constitutionnel de la légalité, consacré par l'article 1, paragraphe (5) de la Constitution. Les critères en fonction desquels s'effectue la sélection des infrastructures cybernétiques d'intérêt national et la manière dont ils sont fixés doivent être prévus par la loi, et l'acte normatif de réglementation primaire doit comporter une liste aussi exhaustive que possible des domaines auxquels s'appliquent les dispositions légales.

La Cour a également jugé que les obligations découlant de la Loi sur la cybersécurité de la Roumanie devaient être applicables exclusivement aux personnes morales de droit public ou privé, détenteurs ou ayant sous leur responsabilité des ICIN (qui comprennent aussi, en vertu de la loi, les administrations publiques), étant donné que seules les situations de danger sur une infrastructure d'intérêt national peuvent avoir des répercussions sur la sécurité de la Roumanie. Or, les dispositions légales dans la version soumise au contrôle de constitutionnalité présentent un très haut degré de généralité, les obligations visant tous les détenteurs d'infrastructures cybernétiques, consistant dans des systèmes informatiques, les applications afférentes, des réseaux et des services de communications électroniques, quelle que soit leur importance qui peut porter sur l'intérêt national ou seulement sur un intérêt de groupe ou bien particulier. Pour les raisons exposées ci-dessus, les dispositions de la Loi sur la cybersécurité de la Roumanie violent les dispositions de l'article 1, paragraphe (5) de la Constitution, ne répondant pas aux exigences de prévisibilité, stabilité et certitude.

La Cour a également retenu que, conformément aux dispositions de l'article 20, paragraphe (1), point c) de la loi, les personnes morales de droit public ou privé détenant ou ayant sous leur responsabilité les ICIN étaient tenues d'autoriser la production d'audits de cybersécurité sur demande motivée des autorités compétentes. Les audits sont réalisés par le SRI ou par les prestataires de services de cybersécurité. En d'autres termes, étant donné que le SRI est l'autorité nationale en matière de cybersécurité, donc l'autorité compétente, conformément à la loi, de demander aux personnes morales de droit public ou privé détenant ou ayant sous leur responsabilité des ICIN d'effectuer des audits de cybersécurité, il y a une réelle possibilité que cette institution se trouve simultanément dans la position du demandeur de l'audit, de celui qui procède à l'audit, de celui auquel on communique le résultat de l'audit et, enfin, dans la position de celui qui constate une éventuelle contravention, conformément à l'article 28, point e), de la loi,

et qui applique la sanction, selon l'article 30, point c) de la loi. Or, une telle situation est inacceptable dans une société régie par les principes de l'État de droit. La Cour a estimé que l'audit devait être réalisé par des auditeurs internes ou par un organisme indépendant, qualifié pour vérifier la conformité de l'application des politiques de cybersécurité au niveau des infrastructures cybernétiques et pour transmettre le résultat de l'évaluation effectuée à l'autorité compétente ou au point de contact unique.

La Cour a aussi retenu de l'analyse de la loi que celle-ci ignorait de régir la possibilité des sujets destinataires de la loi, à la charge desquels on a instauré des obligations et des responsabilités, de contester en justice les actes administratifs conclus quant à la satisfaction de ces obligations et étant susceptibles de porter atteinte à un droit ou un intérêt légitime. L'absence de toute indication dans le contenu de la loi garantissant la possibilité de la personne dont les droits, libertés et intérêts légitimes ont été lésés par des actes ou des faits reposant sur les dispositions de la Loi sur la cybersécurité de la Roumanie de s'adresser à une instance judiciaire indépendante et impartiale constitue une violation des dispositions constitutionnelles de l'article 1, paragraphes (3) et (5) et de l'article 21, ainsi que de l'article 6 de la Convention de sauvegarde des Droits de l'Homme et des Libertés Fondamentales.

De même, le choix du législateur d'attribuer des compétences de surveillance et de contrôle de l'application des dispositions légales à la Chambre des Députés, au Sénat, à l'Administration Présidentielle, au Secrétariat Général du Gouvernement et au CSAT, alors que l'article 10, paragraphes (1) et (2) prévoit les autorités compétentes en matière de cybersécurité concernant les infrastructures cybernétiques propres ou celles sous leur responsabilité, sans inclure dans cette catégorie les autorités énumérées ci-dessus, celles-ci se retrouvant dans l'ensemble de l'acte normatif dans la catégorie des personnes morales de droit public, chargées du respect des obligations prévues par la loi, témoigne d'une incohérence et prête à confusion quant au régime juridique applicable à ces institutions. Ainsi, en vertu de la loi critiquée, le Parlement, l'Administration Présidentielle, le Gouvernement ou le CSAT, autorités de rang constitutionnel dont les attributions sont expressément prévues dans la loi fondamentale, subrogent dans des attributions qui incombent à la compétence des autorités de l'administration publique centrale ou locale, deviennent des agents verbalisateurs de la commission de contraventions et ordonnent l'application de sanctions contraventionnelles. La Cour a constaté qu'une telle réglementation démontrait ignorer les principes de droit régissant un État démocratique, à savoir le principe de la

séparation des pouvoirs au sein de l'État, prévu à l'article 1, paragraphe (4) de la Constitution, et le principe de la légalité, consacré par l'article 1, paragraphe (5).

Enfin, la Cour a également constaté que l'ensemble de l'acte normatif présentait des lacunes en matière du respect des règles de technique législative, de la cohérence, de la clarté, de la prévisibilité, susceptible d'engendrer une violation du principe de la légalité, consacré par l'article 1, paragraphe (5) de la Constitution. Ainsi, la loi fait référence dans plusieurs cas à la réglementation de certains aspects essentiels dans l'économie de la matière régie, à la législation secondaire, tels des arrêtés du Gouvernement, des normes méthodologiques, des ordres ou des décisions ou « des procédures convenues ».

III. La Cour a fait droit à l'exception d'inconstitutionnalité et a constaté que la Loi sur la cybersécurité de la Roumanie était inconstitutionnelle dans son ensemble.