Recommandations 02/2020 sur les garanties essentielles européennes pour les mesures de surveillance

Adoptées le 10 novembre 2020

Table des matières

Le comité européen de la protection des données

Vu l'article 70, paragraphe 1, point e), du 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 (ci-après le «RGPD»)[1],

Vu l'accord sur l'Espace économique européen (EEE) et, en particulier, son annexe XI et son protocole 37, tels que modifiés par la décision du Comité mixte de l'EEE nº 154/2018 du 6 juillet 2018[2],

Vu les articles 12 et 22 de son règlement intérieur,

Vu le document de travail du groupe de travail « Article 29» sur la justification des ingérences dans les droits fondamentaux au respect de la vie privée et à la protection des données par des mesures de surveillance lors du transfert de données à caractère personnel («garanties essentielles européennes», WP237),

A ADOPTÉ LES RECOMMANDATIONS SUIVANTES:

1. INTRODUCTION

1. À la suite de l'arrêt Schrems I, les autorités de l'UE chargées de la protection des données réunies au sein du groupe de travail «Article 29» se sont appuyées sur la jurisprudence pour recenser les garanties essentielles européennes à respecter afin que les ingérences dans les droits fondamentaux au respect de la vie privée et à la protection des données par le biais de mesures de surveillance lors du transfert de données à caractère personnel n'aillent pas au-delà de ce qui est nécessaire et proportionné dans une société démocratique.

2. Le comité européen de la protection des données tient à souligner que les garanties essentielles européennes reposent sur la jurisprudence de la Cour de justice de l'Union européenne (ci-après la «CJUE») concernant les articles 7, 8, 47 et 52 de la Charte des droits fondamentaux de l'Union européenne (ci-après la «Charte») et, le cas échéant, sur la jurisprudence de la Cour européenne des droits de l'homme (ci-après la «CouEDH») relative à l'article 8 de la Convention européenne des droits de l'homme (ci-après la «CEDH») concernant les questions de surveillance dans les États parties à la CEDH[3].

[1] Le présent document ne concerne pas les cas de transferts ou de transferts ultérieurs relevant du champ d'application de la directive en matière de protection des données dans le domaine répressif [directive (UE) 2016/680].

[2] Dans le présent document, on entend par « États membres» les «États membres de l'EEE».

[3] Dans les présentes recommandations, l'expression « droits fondamentaux» trouve son origine dans la Charte des droits fondamentaux de l'Union européenne. Elle s'entend toutefois également des « droits de l'homme», tels qu'ils sont consacrés par la Convention européenne des droits de l'homme.

3. La mise à jour du présent document vise à préciser davantage les garanties essentielles européennes élaborées à l'origine en réponse à l'arrêt Schrems I[4], en tenant compte des clarifications apportées par la CJUE (et par la CouEDH) depuis sa publication, notamment dans son arrêt phare Schrems II[5].

4. Dans son arrêt Schrems II, la CJUE a déclaré que l'examen de la décision 2010/87/UE de la Commission relative aux clauses contractuelles types pour le transfert de données à caractère personnel vers des sous-traitants établis dans des pays tiers, à la lumière des articles 7, 8 et 47 de la Charte, n'avait révélé aucun élément de nature à affecter la validité de cette décision, mais elle a invalidé la décision relative au « bouclier de protection des données» (ci-après la «décision BPD»). La CJUE a déclaré que la décision BPD était incompatible avec l'article 45, paragraphe 1, du RGPD, lu à la lumière des articles 7, 8 et 47 de la Charte. L'arrêt peut donc servir d'exemple lorsque des mesures de surveillance prises dans un pays tiers (en l'occurrence, les États-Unis, avec l'article 702 du FISA et le décret présidentiel nº 12 333) ne sont pas suffisamment limitées et ne sont pas susceptibles d'un recours effectif permettant aux personnes concernées de faire valoir leurs droits, comme l'exige le droit de l'Union pour considérer que le niveau de protection dans le pays tiers est «essentiellement équivalent» à celui qui est garanti dans l'Union, au sens de l'article 45, paragraphe 1, du RGPD.

5. Les raisons de l'invalidation du bouclier de protection des données ont également eu des conséquences sur d'autres outils de transfert[6]. Bien que la Cour ait interprété l'article 46, paragraphe 1, du RGPD dans le contexte de la validité des clauses contractuelles types (ci-après les «CCT»), son interprétation s'applique à tout transfert vers des pays tiers au moyen de l'un des outils visés à l'article 46 du RGPD[7].

6. En dernier ressort, il appartient à la CJUE de juger si des ingérences dans un droit fondamental peuvent être justifiées. Toutefois, en l'absence d'un tel jugement et conformément à la jurisprudence actuelle, les autorités chargées de la protection des données sont tenues d'évaluer les cas individuels, soit d'office, soit à la suite d'une plainte, et de renvoyer l'affaire devant une juridiction nationale si elles soupçonnent que le transfert n'est pas conforme à l'article 45 dans le cas d'une décision d'adéquation, ou de suspendre ou interdire le transfert si elles estiment qu'il n'est pas possible de respecter l'article 46 du RGPD et que la protection des données transférées que requiert le droit de l'Union ne peut pas être assurée par d'autres moyens.

7. Les garanties essentielles européennes mises à jour ont pour but de fournir des éléments permettant de déterminer si des mesures de surveillance autorisant l'accès d'autorités publiques d'un pays tiers à des données à caractère personnel, qu'il s'agisse d'agences de sécurité nationale ou d'autorités répressives, peuvent être considérées comme une ingérence justifiable ou non.

8. En effet, les garanties essentielles européennes font partie de l'évaluation à réaliser afin de déterminer si un pays tiers offre un niveau de protection essentiellement équivalent à celui qui est garanti au sein de l'Union, mais elles n'ont pas en soi pour objectif de définir tous les éléments

[4] Arrêt de la CJUE du 6 octobre 2015, Maximillian Schrems/Data Protection Commissioner, C-362/14, EU:C:2015:650 (ci-après « Schrems I»).

[5] Arrêt de la CJUE du 16 juillet 2020, Data Protection Commissioner/Facebook Ireland Ltd, Maximillian Schrems, C-311/18, ECLI:EU:C:2020:559 (ci-après « Schrems II»).

[6] Schrems II, § 105.

[7] Schrems II, § 92.

nécessaires pour considérer qu'un pays tiers offre ce niveau de protection conformément à l'article 45 du RGPD. De même, elles ne visent pas, en soi, à définir tous les éléments qu'il conviendrait de prendre en considération pour apprécier si le régime juridique d'un pays tiers empêche l'exportateur et l'importateur des données de fournir des garanties appropriées conformément à l'article 46 du RGPD.

9. Par conséquent, les éléments décrits dans le présent document devraient être considérés comme étant les garanties essentielles qui doivent être trouvées dans le pays tiers lors de l'évaluation de l'ingérence, découlant des mesures de surveillance dudit pays, dans les droits au respect de la vie privée et à la protection des données, plutôt que comme une liste d'éléments visant à démontrer que le régime juridique d'un pays tiers dans son ensemble assure un niveau de protection essentiellement équivalent.

10. L'article 6, paragraphe 3, du traité sur l'Union européenne dispose que les droits fondamentaux énoncés dans la CEDH constituent des principes généraux du droit de l'Union. Toutefois, comme le rappelle la CJUE dans sa jurisprudence, la CEDH ne constitue pas, tant que l'Union n'y a pas adhéré, un instrument juridique formellement intégré à l'ordre juridique de l'Union[8]. Dès lors, le niveau de protection des droits fondamentaux exigé par l'article 46, paragraphe 1, du RGPD doit être déterminé sur la base des dispositions dudit règlement, lues à la lumière des droits fondamentaux consacrés par la Charte. Cela étant, conformément à l'article 52, paragraphe 3, de la Charte, les droits contenus dans cette dernière et les droits correspondants garantis par la CEDH doivent avoir la même signification et la même portée que ceux énoncés dans ladite convention et, partant, comme l'a rappelé la CJUE, il convient de tenir compte de la jurisprudence de la CouEDH relative aux droits déjà prévus dans la Charte des droits fondamentaux de l'Union européenne en tant que seuil de protection minimale en vue de l'interprétation des droits correspondants de la Charte[9]. Toutefois, conformément à l'article 52, paragraphe 3, dernière phrase, de la Charte, «[c]ette disposition ne fait pas obstacle à ce que le droit de l'Union accorde une protection plus étendue».

11. Dès lors, la teneur des garanties essentielles continuera de s'appuyer en partie sur la jurisprudence de la CouEDH, dans la mesure où la Charte telle qu'interprétée par la CJUE n'offre pas un niveau de protection supérieur imposant d'autres exigences que la jurisprudence de la CouEDH.

12. Le présent document situe le contexte et précise les quatre garanties essentielles européennes.

2. INGÉRENCES DANS LES DROITS FONDAMENTAUX

13. Les droits fondamentaux au respect de la vie privée et familiale, y compris les communications, et à la protection des données à caractère personnel sont énoncés aux articles 7 et 8 de la Charte et s'appliquent à toute personne. L'article 8 précise les conditions de la licéité du traitement des données à caractère personnel, reconnaît le droit d'accès et de rectification et exige que le respect de ces règles soit soumis au contrôle d'une autorité indépendante.

[8] Schrems II, § 98.

[9] Affaires jointes C-511/18, C-512/18 et C-520/18, La Quadrature du Net e.a. (ci-après « La Quadrature du Net e.a.»).

14. «[L]'opération consistant à faire transférer des données à caractère personnel d'un État membre vers un pays tiers constitue, en tant que telle, un traitement de données à caractère personnel»[10]. Par conséquent, les articles 7 et 8 de la Charte s'appliquent à cette opération spécifique et leur protection s'étend aux données transférées, raison pour laquelle les personnes concernées dont les données à caractère personnel sont transférées vers un pays tiers doivent bénéficier d'un niveau de protection essentiellement équivalent à celui garanti au sein de l'Union[11].

15. Selon la CJUE, lorsque le traitement des données à caractère personnel d'une personne physique porte atteinte au droit fondamental au respect de la vie privée consacré à l'article 7 de la Charte, il y a également atteinte au droit à la protection des données, étant donné que ce traitement relève du champ d'application de l'article 8 de la Charte et doit, dès lors, nécessairement satisfaire à l'exigence de protection des données prévue audit article[12].

16. Par conséquent, s'agissant de l'ingérence possible dans les droits fondamentaux consacrés dans le droit de l'Union, l'obligation imposée aux fournisseurs de services de communications électroniques (...) de conserver les données relatives au trafic aux fins de les rendre, le cas échéant, accessibles aux autorités nationales compétentes soulève des questions relatives au respect des articles 7 et 8 de la Charte[13.]. Ces mêmes questions se posent également pour d'autres types de traitement de données, tels que leur transmission à des personnes autres que les utilisateurs ou l'accès à ces données en vue de leur utilisation[14], ce qui implique donc une ingérence dans ces droits fondamentaux. En outre, l'accès aux données par une autorité publique constitue une ingérence supplémentaire, conformément à une jurisprudence constante[15].

17. Pour constater une ingérence, il importe peu de «savoir si les informations relatives à la vie privée concernée présentent ou non un caractère sensible, ou si les intéressés ont ou non subi d'éventuels inconvénients en raison de cette ingérence»[16]. La CJUE a également souligné que la question de savoir si les données conservées ont été utilisées ou non est dénuée de pertinence[17].

18. Toutefois, les droits consacrés aux articles 7, 8 et 11 de la Charte n'apparaissent pas comme étant des prérogatives absolues, mais doivent être pris en considération par rapport à leur fonction dans la société[18].

19. La Charte inclut un critère de nécessité et de proportionnalité pour encadrer les limitations aux droits qu'elle protège. Son article 52, paragraphe 1, précise la portée des limitations possibles aux articles 7 et 8 en disposant que « toute limitation de l'exercice des droits et libertés reconnus par la présente Charte doit être prévue par la loi et respecter le contenu essentiel desdits droits et libertés. Dans le respect du principe de proportionnalité, des limitations ne peuvent être apportées que si elles

[10] CJUE, Schrems II, § 83.
[11] CJUE, Schrems II, § 96.
[12] CJUE, Schrems II, § 170-171.
[13] CJUE, C-623/17, Privacy International (ci-après « Privacy International»), § 60.
[14] CJUE, Privacy International, § 61.
[15] CouEDH, Leander, § 48; CouEDH, Rotaru, § 46; CJUE, Digital Rights Ireland, § 35.
[16] CJUE, Schrems II, § 171 et jurisprudence citée.
[17] CJUE, Schrems II, § 171 et jurisprudence citée.
[18] CJUE, Privacy International, § 63.

sont nécessaires et répondent effectivement à des objectifs d'intérêt général reconnus par l'Union ou au besoin de protection des droits et libertés d'autrui ».

20. La CJUE a rappelé qu'une législation de l'Union qui implique une ingérence dans les droits fondamentaux garantis par les articles 7 et 8 de la Charte « doit prévoir des règles claires et précises régissant la portée et l'application de la mesure en cause et imposant des exigences minimales, de telle sorte que les personnes dont les données à caractère personnel sont concernées disposent de garanties suffisantes permettant de protéger efficacement ces données contre les risques d'abus », notamment lorsque les données à caractère personnel sont soumises à un traitement automatisé et «lorsqu'il existe un risque important d'accès illicite à ces données »[19].

21. Selon la CJUE, la protection du droit au respect de la vie privée impose que les dérogations et les limitations au droit à la protection des données « s'opèrent dans les limites du strict nécessaire». En outre, un objectif d'intérêt général doit se concilier avec les droits fondamentaux concernés par la mesure en «effectuant une pondération équilibrée» entre cet objectif et les droits en cause[20].

22. Il en résulte que l'accès, la conservation et l'utilisation ultérieure de données à caractère personnel par des autorités publiques dans le cadre de mesures de surveillance ne doivent pas excéder les limites du strict nécessaire, appréciées à la lumière de la Charte, sans quoi «elle[s] ne saurai[en]t être considérée[s] comme étant justifiée[s], dans une société démocratique»[21].

23. Les quatre garanties essentielles européennes, telles qu'elles sont détaillées dans la section suivante, visent à préciser comment il convient d'apprécier le niveau d'ingérence dans les droits fondamentaux au respect de la vie privée et à la protection des données dans le cadre de mesures de surveillance adoptées par des autorités publiques d'un pays tiers, lors du transfert de données à caractère personnel, et quelles prescriptions légales doivent s'appliquer pour déterminer si ces ingérences seraient acceptables en vertu de la Charte.

3. LES GARANTIES ESSENTIELLES EUROPÉENNES

24. À la suite de l'analyse de la jurisprudence, le comité européen de la protection des données considère que les exigences légales applicables pour justifier les limitations aux droits au respect de la vie privée et à la protection des données reconnus par la Charte peuvent se résumer à quatre garanties essentielles européennes :

A. Le traitement doit reposer sur des règles claires, précises et accessibles;
B. La nécessité et la proportionnalité du traitement au regard des objectifs légitimes poursuivis doivent être démontrées;
C. Un mécanisme de surveillance indépendant doit être mis en place;
D. L'intéressé doit disposer de voies de recours effectives.

25. Ces garanties reposent sur les droits fondamentaux au respect de la vie privée et à la protection des données dont bénéficie toute personne, quelle que soit sa nationalité.

[19] CJUE, Privacy International, § 68 et jurisprudence citée.
[20] CJUE, Privacy International, § 68 et jurisprudence citée.
[21] CJUE, Privacy International, § 81.

Garantie A – Le traitement doit reposer sur des règles claires, précises et accessibles

26. Conformément à l'article 8, paragraphe 2, de la Charte, les données à caractère personnel doivent être traitées à des fins déterminées et sur la base du consentement de la personne concernée ou en vertu d'un autre fondement légitime prévu par la loi »[22], comme l'a rappelé la CJUE dans l'arrêt Schrems II. Par ailleurs, aux termes de l'article 52, paragraphe 1, de la Charte, toute limitation de l'exercice des droits et libertés reconnus par la Charte dans l'Union doit être prévue par la loi. Une ingérence justifiable doit donc être conforme à la loi.

27. Ce fondement juridique doit prévoir des règles claires et précises régissant la portée et l'application de la mesure en cause et imposant des exigences minimales[23]. En outre, la Cour a rappelé que cette «réglementation doit être légalement contraignante en droit interne»[24]. À cet égard, la CJUE a précisé que l'appréciation du droit applicable du pays tiers doit porter sur la question de savoir si la personne concernée peut l'invoquer et s'en prévaloir devant les tribunaux[25]. La Cour indique donc que les droits conférés aux personnes concernées doivent être effectifs; lorsqu'elles ne bénéficient pas de droits opposables aux autorités publiques, le niveau de protection assuré ne saurait être considéré comme étant essentiellement équivalent à celui résultant de la Charte, contrairement à ce qu'exige l'article 45, paragraphe 2, point a), du RGPD[26].

28. Par ailleurs, la Cour a souligné que le droit applicable doit indiquer en quelles circonstances et sous quelles conditions une mesure prévoyant le traitement de telles données peut être prise[27] (voir sous le point « Garantie B », *infra*, le rapport entre ces exigences et les principes de nécessité et de proportionnalité).

29. De plus, la CJUE a également déclaré que « l'exigence selon laquelle toute limitation de l'exercice des droits fondamentaux doit être prévue par la loi implique que la base légale qui permet l'ingérence dans ces droits doit définir elle-même la portée de la limitation de l'exercice du droit concerné »[28].

30. Enfin, la Cour européenne des droits de l'homme « ne voit aucune raison de soumettre les règles gouvernant l'interception des communications individuelles et les dispositifs de surveillance plus généraux à des critères d'accessibilité et de clarté différents »[29]. La CouEDH a également précisé que la base légale doit à tout le moins contenir une définition des catégories de personnes susceptibles de faire l'objet d'une surveillance, une limite à la durée de l'exécution de la mesure, la procédure à suivre pour l'examen, l'utilisation et la conservation des données recueillies et les précautions à prendre pour la communication des données à d'autres parties[30].

---

[22] Schrems II, § 173.

[23] Schrems II, § 175, 180, et avis 1/15 (Accord PNR UE-Canada) du 26 juillet 2017, § 139 et jurisprudence citée.

[24] Privacy International, § 68. Il devrait également être clair que, dans la version française de l'arrêt, la Cour utilise le terme « réglementation», qui est plus large que les seuls actes du Parlement.

[25] Schrems II, § 181, où la Cour fait référence à la Presidential Policy Directive 28 des États-Unis.

[26] Schrems II, § 181.

[27] Privacy International, § 68, concernant le droit des États membres.

[28] Schrems II, § 175 et jurisprudence citée; Privacy International, § 65.

[29] CouEDH, Liberty, § 63.

[30] CouEDH, Weber et Saravia, § 95.

31. Enfin, l'ingérence doit être prévisible quant à ses effets pour l'intéressé afin de lui garantir une protection adéquate et effective contre une ingérence arbitraire et le risque d'abus. Il en résulte que le traitement doit reposer sur une base juridique précise, claire, mais également accessible (à savoir publique)[31]. Sur cette question, la CouEDH a rappelé dans l'affaire Zakharov qu' « en matière d'interception de communications, la "prévisibilité" ne pouvait se comprendre de la même façon que dans beaucoup d'autres domaines». Elle a indiqué que, dans le contexte particulier des mesures de surveillance secrète, telle l'interception de communications, « la prévisibilité ne saurait signifier qu'un individu doit se trouver à même de prévoir quand les autorités sont susceptibles d'intercepter ses communications de manière qu'il puisse adapter sa conduite en conséquence ». Or, étant donné que dans ce type de situation, le risque d'arbitraire apparaît avec netteté, « l'existence de règles claires et détaillées en matière d'interception de conversations téléphoniques apparaît donc indispensable, d'autant que les procédés techniques utilisables ne cessent de se perfectionner. La loi doit être rédigée avec suffisamment de clarté pour indiquer à tous de manière adéquate en quelles circonstances et sous quelles conditions elle habilite la puissance publique à prendre pareilles mesures secrètes»[32].

Garantie B – La nécessité et la proportionnalité du traitement au regard des objectifs légitimes poursuivis doivent être démontrées

32. Conformément à l'article 52, paragraphe 1, première phrase, de la Charte, toute limitation de l'exercice des droits et libertés reconnus par la charte doit respecter le contenu essentiel desdits droits et libertés. En vertu de l'article 52, paragraphe 1, seconde phrase, de la Charte, dans le respect du principe de proportionnalité, des limitations ne peuvent être apportées à ces droits et libertés que si elles sont nécessaires et répondent effectivement à des objectifs d'intérêt général reconnus par l'Union ou au besoin de protection des droits et des libertés d'autrui[33].

33. S'agissant du **principe de proportionnalité**, la Cour a déclaré, au sujet de la réglementation des États membres, que la possibilité de justifier une limitation aux droits au respect de la vie privée et à la protection des données doit être appréciée, d'une part, en mesurant la **gravité de l'ingérence** que comporte une telle limitation[34] et, d'autre part, en vérifiant que **l'importance de l'objectif d'intérêt général** poursuivi par cette limitation est en relation avec cette gravité[35].

34. Dans l'arrêt La Quadrature du Net e.a., il convient d'observer que, s'agissant de la réglementation d'un État membre et non celle d'un pays tiers, la CJUE a déclaré que l'importance de l'objectif de sauvegarde de la sécurité nationale est susceptible de justifier des mesures comportant des ingérences dans les droits fondamentaux plus graves que celles que pourraient justifier d'autres objectifs, tels que la lutte contre la criminalité. Elle a toutefois conclu qu'il en est ainsi dès lors qu'il existe des circonstances suffisamment concrètes permettant de considérer que l'État membre concerné fait face à une menace

[31] CouEDH, Malone, § 65-66.

[32] CouEDH, Zakharov, § 229.

[33] Schrems II, § 174.

[34] Dans ce contexte, la Cour a notamment relevé que « l'ingérence que comporte le recueil en temps réel des données permettant de localiser un équipement terminal apparaît particulièrement grave, dès lors que ces données fournissent aux autorités nationales compétentes le moyen d'un suivi précis et permanent des déplacements des utilisateurs des téléphones mobiles (...)» (La Quadrature du Net e.a., § 187 et jurisprudence citée).

[35] La Quadrature du Net e.a., § 131.

grave pour la sécurité nationale qui s'avère réelle et actuelle ou prévisible et satisfait aux autres exigences énoncées à l'article 52, paragraphe 1, de la Charte[36].

35. À cet égard, conformément à la jurisprudence constante de la Cour, les dérogations et limitations à la protection des données à caractère personnel ne doivent s'opérer que dans les limites du strict nécessaire[37]. Pour satisfaire à cette exigence, outre l'établissement de règles claires et précises régissant la portée et l'application de la mesure en cause, la réglementation en cause doit imposer des exigences minimales, de sorte que les personnes dont les données ont été transférées disposent de garanties suffisantes permettant de protéger efficacement leurs données à caractère personnel contre les risques d'abus. « Elle doit en particulier indiquer en quelles circonstances et sous quelles conditions une mesure prévoyant le traitement de telles données peut être prise, garantissant ainsi que l'ingérence soit limitée au strict nécessaire. La nécessité de disposer de telles garanties est d'autant plus importante lorsque les données à caractère personnel sont soumises à un traitement automatisé »[38].

36. Dans l'arrêt Schrems II, la CJUE a souligné que la législation d'un pays tiers qui ne fait ressortir d'aucune manière l'existence de limitations à l'habilitation qu'elle comporte pour la mise en œuvre des programmes de surveillance aux fins du renseignement extérieur ne saurait assurer un niveau de protection substantiellement équivalent à celui garanti par la Charte. En effet, selon la jurisprudence, une base légale qui permet des ingérences dans les droits fondamentaux doit, pour satisfaire au principe de proportionnalité, définir elle-même la portée de la limitation de l'exercice du droit concerné[39].

37. S'agissant du **principe de nécessité**, la CJUE a indiqué qu'une réglementation «qui autorise de manière généralisée la conservation de l'intégralité des données à caractère personnel de toutes les personnes dont les données ont été transférées depuis l'Union (...) sans qu'aucune différenciation, limitation ou exception soit opérée en fonction de l'objectif poursuivi et sans que soit prévu un critère objectif permettant de délimiter l'accès des autorités publiques aux données et leur utilisation ultérieure à des fins précises, strictement restreintes et susceptibles de justifier l'ingérence que comportent tant l'accès que l'utilisation de ces données» n'est pas conforme à ce principe[40]. En particulier, une réglementation permettant aux autorités publiques d'accéder de manière généralisée

[36] § 136-137. Voir également Privacy International. Comme la Cour l'a précisé, ces menaces se distinguent, par leur nature et leur particulière gravité, du risque général de survenance de tensions ou de troubles, même graves, à la sécurité publique (§ 75). À titre d'exemple, dans l'arrêt La Quadrature du Net e.a., la Cour a relevé que l'ingérence résultant d'une analyse automatisée des données relatives au trafic et des données de localisation s'avère particulièrement grave dès lors qu'elle couvre de manière généralisée et indifférenciée les données des personnes faisant usage des moyens de communications électroniques, de sorte que cette mesure ne peut satisfaire à l'exigence de proportionnalité que dans des situations dans lesquelles l'État membre concerné se trouve face à une menace grave pour la sécurité nationale qui s'avère réelle et actuelle ou prévisible et, entre autres conditions, à la condition que la durée de cette conservation soit limitée au strict nécessaire (§ 174-177).

[37] Schrems II, § 176 et jurisprudence citée.

[38] Schrems II, § 175.

[39] Schrems II, § 180.

[40] Schrems I, § 93 avec d'autres références. Voir, toutefois, en ce qui concerne la réglementation d'un État membre et non celle d'un pays tiers, Privacy International, § 71 et jurisprudence citée. Dans cette affaire, la Cour a déclaré qu'une réglementation nationale imposant aux fournisseurs de services de communications électroniques de procéder à la communication par transmission généralisée et indifférenciée des données relatives au trafic et des données de localisation aux services de sécurité et de renseignement, excède les limites du strict nécessaire et ne saurait être considérée comme étant justifiée, dans une société démocratique, ainsi que l'exige la directive vie privée et communications électroniques, lue à l'aune de la Charte (§ 81).

au contenu de communications électroniques doit être considérée comme portant atteinte au contenu essentiel du droit fondamental au respect de la vie privée, tel que garanti par l'article 7 de la Charte[41].

38. De même, cette fois dans le cadre de l'évaluation d'une réglementation d'un État membre et non d'un pays tiers, la CJUE a déclaré dans l'arrêt La Quadrature du Net e.a. qu'«une réglementation prévoyant une conservation des données à caractère personnel doit toujours répondre à des critères objectifs, établissant un rapport entre les données à conserver et l'objectif poursuivi»[42]. Dans le même contexte, dans l'arrêt Privacy International, la Cour a également conclu que le législateur «doit se fonder sur des critères objectifs pour définir les circonstances et les conditions dans lesquelles doit être accordé aux autorités nationales compétentes l'accès aux données en cause»[43].

Garantie C – Mécanisme de surveillance indépendant

39. Le comité européen de la protection des données rappelle qu'une ingérence a lieu au moment de la collecte des données, mais aussi au moment où une autorité publique accède à des données en vue de leur traitement ultérieur. La CouEDH a précisé à maintes reprises que toute ingérence dans le droit au respect de la vie privée et à la protection des données doit être soumise à un mécanisme de surveillance efficace, indépendant et impartial, qui doit être assuré par un juge ou par un autre organe indépendant[44] (comme une autorité administrative ou un organe parlementaire). Dans l'arrêt Schrems II, la CJUE a également tenu compte du contrôle de l'application des mesures de surveillance par un organe indépendant[45].

40. La CouEDH précise que si l'autorisation (judiciaire) préalable des mesures de surveillance est certes une garantie importante contre l'arbitraire, il faut également apprécier le fonctionnement correct du système d'interception, en tenant compte de l'existence ou de l'absence de freins et de contrepoids à l'exercice du pouvoir et de signes d'abus réels[46]. Dans l'arrêt Schrems II, la CJUE a également tenu compte de la portée du rôle du mécanisme de surveillance, qui ne couvrait pas les mesures de surveillance individuelle[47].

---

[41] Schrems I, § 94.

[42] La Quadrature du Net e.a., § 133. Dans ce contexte, la Cour a confirmé que la directive vie privée et communications électroniques, lue à la lumière de la Charte, s'oppose à des mesures législatives prévoyant, à titre préventif, une conservation générale et indifférenciée des données relatives au trafic et des données de localisation. En revanche, la Cour a estimé que le législateur ne s'oppose pas, dans des situations de menace grave pour la sécurité nationale qui s'avère réelle et actuelle ou prévisible, au recours à une injonction faite aux fournisseurs de services de communications électroniques de procéder à une conservation généralisée et indifférenciée des données relatives au trafic et des données de localisation. Cette mesure doit toutefois respecter des conditions spécifiques. En particulier, l'injonction ne peut être émise que pour une période temporellement limitée au strict nécessaire, mais renouvelable en cas de persistance de la menace (§ 168).

[43] Privacy International, § 78 et jurisprudence citée. Dans l'arrêt Privacy International, s'agissant de l'accès d'une autorité à des données à caractère personnel prévu par la réglementation d'un État membre, la Cour a jugé qu'« un accès général à toutes les données conservées, en l'absence de tout lien, même indirect, avec le but poursuivi, ne peut être considéré comme étant limité au strict nécessaire» (§ 77-78).

[44] CouEDH, Klass, § 17, 51.

[45] Schrems II, § 179, 183.

[46] CouEDH, Big Brother Watch, § 319-320, appel pendant.

[47] Schrems II, § 179.

41. En ce qui concerne la législation des États membres, la CJUE a recensé un certain nombre de mesures qui ne sont conformes au droit de l'Union que si elles sont soumises à un contrôle effectif exercé soit par une juridiction, soit par une entité administrative indépendante, dont la décision est dotée d'un effet contraignant. L'objet de ce contrôle est de vérifier l'existence d'une situation justifiant la mesure et le respect des conditions et des garanties devant être prévues[48]. En ce qui concerne le recueil en temps réel des données relatives au trafic et des données de localisation, le contrôle doit notamment permettre de s'assurer au préalable qu'un tel recueil n'est autorisé que dans la limite de ce qui est strictement nécessaire. En cas d'urgence dûment justifiée, les mesures peuvent avoir lieu sans un tel contrôle préalable; toutefois, la Cour impose toujours que le contrôle postérieur intervienne dans un délai bref[49].

42. Quant à l'indépendance des mécanismes de contrôle en matière de surveillance, les conclusions de la CJUE concernant l'indépendance d'une entité dans le cadre du recours pourraient être prises en considération (voir sous le point « Garantie D», *infra*). En outre, la jurisprudence de la CouEDH peut apporter des éléments supplémentaires. Cette Cour a estimé préférable que le contrôle soit confié à un juge. Il n'est toutefois pas exclu qu'un autre organe puisse être responsable «à condition que cet organe soit suffisamment indépendant à l'égard de l'exécutif»[50] et «des autorités qui procèdent à la surveillance; [il est] investi de pouvoirs et attributions suffisants pour exercer un contrôle efficace et permanent»[51]. La CouEDH a ajouté que «le mode de désignation et le statut juridique des membres de l'organe de contrôle»[52] doivent être pris en compte pour apprécier l'indépendance. Cela inclut des « personnes possédant les qualifications requises pour accéder à la magistrature et nommées soit par le parlement soit par le Premier ministre. En revanche, elle a jugé insuffisamment indépendant un ministre de l'intérieur qui non seulement était nommé par le pouvoir politique et membre de l'exécutif, mais de plus était directement impliqué dans la commande de moyens spéciaux de surveillance»[53]. Selon la CouEDH, «il est essentiel que l'organe de contrôle ait accès à tous les documents pertinents, y compris à des informations confidentielles»[54]. Enfin, la CouEDH recherche «si les activités de l'organe de contrôle sont ouvertes à un droit de regard du public»[55].

Garantie D - L'intéressé doit disposer de voies de recours effectives

43. La dernière garantie essentielle européenne a trait au droit de toute personne à des voies de recours. Celle-ci doit disposer d'un recours effectif pour faire valoir ses droits lorsqu'elle estime qu'ils ne sont pas ou n'ont pas été respectés. Dans l'arrêt Schrems I, la CJUE a expliqué qu'« une réglementation ne prévoyant aucune possibilité pour le justiciable d'exercer des voies de droit afin d'avoir accès à des données à caractère personnel le concernant, ou d'obtenir la rectification ou la suppression de telles données, ne respecte pas le contenu essentiel du droit fondamental à une protection juridictionnelle effective, tel que consacré à l'article 47 de la Charte. L'article 47, premier alinéa, de la Charte exige que toute personne dont les droits et libertés garantis par le droit de l'Union

[48] CJUE, La Quadrature du Net e.a., § 168, 189.

[49] CJUE, La Quadrature du Net e.a., § 189.

[50] CouEDH, Zakharov, § 258, Iordachi e.a. c. Moldova, § 40, 51; Dumitru Popescu c. Roumanie, § 70-73.

[51] CouEDH, Klass, § 56, Big Brother Watch, § 318, appel pendant.

[52] CouEDH, Zakharov, § 278.

[53] CouEDH, Zakharov, § 278.

[54] CouEDH, Zakharov, § 281.

[55] CouEDH, Zakharov, § 283.

ont été violés ait droit à un recours effectif devant un tribunal dans le respect des conditions prévues à cet article»[56].

44. Lors de l'appréciation de la réglementation d'un État membre autorisant le recueil en temps réel des données relatives au trafic et des données de localisation, la Cour a jugé que l'information est nécessaire «pour permettre à ces personnes d'exercer leurs droits, découlant des articles 7 et 8 de la Charte, de demander l'accès à leurs données à caractère personnel faisant l'objet de ces mesures et, le cas échéant, la rectification ou la suppression de celles-ci, ainsi que d'introduire, conformément à l'article 47, premier alinéa, de la Charte, un recours effectif devant un tribunal»[57]. Elle a néanmoins également reconnu que l'information des personnes dont les données ont été collectées ou analysées ne doit intervenir que pour autant que et qu'à partir du moment où elle n'est pas susceptible de compromettre les missions incombant aux autorités responsables[58].

45. Pour la CouEDH également, la question d'un recours effectif est indissolublement liée à la notification d'une mesure de surveillance à l'intéressé une fois que la surveillance a cessé. En particulier, la Cour a jugé que «la personne concernée ne peut guère, en principe, contester rétrospectivement devant la justice la légalité des mesures prises à son insu, sauf si on l'avise de celles-ci ou si – autre cas de figure –, soupçonnant que ses communications font ou ont fait l'objet d'interceptions, la personne a la faculté de saisir les tribunaux, ceux-ci étant compétents même si le sujet de l'interception n'a pas été informé de cette mesure»[59]. La CouEDH a ainsi reconnu que, dans certains cas, il peut ne pas y avoir de notification, mais qu'un recours effectif doit toutefois être prévu. Ainsi, dans l'affaire Kennedy, par exemple, la Cour a estimé qu'une juridiction offre des voies de recours suffisantes si elle satisfait à une série de conditions, à savoir qu'elle doit être un organe indépendant et impartial, ayant édicté son propre règlement de procédure et composé de membres qui doivent exercer ou avoir exercé de hautes fonctions judiciaires ou être des juristes chevronnés et qu'aucun obstacle probatoire ne doit être surmonté pour saisir cette juridiction[60]. Lorsqu'elle entame l'examen de plaintes de particuliers, la juridiction devrait avoir accès à tous les documents pertinents[61], y compris aux informations confidentielles. Enfin, elle doit être habilitée à agir dans des cas de non-respect[62].

46. L'article 47 de la Charte fait référence à un tribunal, bien que dans d'autres versions linguistiques que le français, la préférence soit donnée au terme «juridiction»[63], tandis que la CEDH impose uniquement aux États membres de s'assurer que «toute personne dont les droits et libertés ont été

[56] CJUE, Schrems I, § 95.
[57] La Quadrature du Net e.a., § 190, et CJUE, avis 1/15, § 220.
[58] La Quadrature du Net e.a., § 191.
[59] CouEDH, Zakharov, § 234.
[60] CouEDH, Kennedy, § 190.
[61] Le comité européen de la protection des données observe que le Commissaire aux droits de l'homme du Conseil de l'Europe estime que la règle dite «des tiers», en vertu de laquelle les services de renseignement d'un pays qui fournissent des données aux services de renseignement d'un autre pays peuvent imposer aux services destinataires de ne pas divulguer les données transférées à un tiers, ne devrait pas s'appliquer aux organes de surveillance afin de ne pas entraver la possibilité d'un recours effectif (Document thématique – La surveillance démocratique et effective des services de sécurité nationale).
[62] CouEDH, Kennedy, § 167.
[63] Le terme « tribunal» est, par exemple, traduit par «Gericht» en allemand et «gerecht» en néerlandais.

violés a droit à l'octroi d'un recours effectif devant une instance nationale»[64], qui ne doit pas nécessairement être une autorité judiciaire[65].

47. Dans l'arrêt Schrems II, lors de l'appréciation du caractère adéquat du niveau de protection d'un pays tiers, la CJUE a rappelé que «les justiciables doivent disposer de la possibilité d'exercer des voies de droit devant un tribunal indépendant et impartial afin d'avoir accès à des données à caractère personnel les concernant, ou d'obtenir la rectification ou la suppression de telles données[66]. Dans le même contexte, la CJUE estime qu'une protection judiciaire effective contre de telles ingérences peut être assurée non seulement par un tribunal, mais également par un organe[67] qui offre des garanties substantiellement équivalentes à celles requises à l'article 47 de la Charte. Dans l'arrêt Schrems II, la CJUE a à la fois souligné que l'indépendance du tribunal ou de l'organe doit être assurée, en particulier par rapport au pouvoir exécutif, assortie de toutes les garanties nécessaires, notamment en ce qui concerne les conditions de sa révocation ou de l'annulation de sa nomination[68], et que les pouvoirs qui devraient être conférés à un tribunal doivent être conformes aux exigences de l'article 47 de la Charte. À cet égard, l'organe[69] sera habilité à prendre des décisions contraignantes à l'égard des services de renseignement, conformément aux garanties légales dont pourraient se prévaloir les personnes concernées[70].

4. OBSERVATIONS FINALES

48. Les quatre garanties essentielles européennes doivent être considérées comme des éléments fondamentaux à rechercher lors de l'appréciation du niveau d'ingérence dans les droits fondamentaux au respect de la vie privée et à la protection des données. Elles ne doivent pas être appréciées indépendamment les unes des autres, dans la mesure où elles sont étroitement liées, mais être considérées globalement, en tenant compte de la législation pertinente en matière de mesures de surveillance, du niveau minimal de garanties pour la protection des droits des personnes concernées et des voies de recours que prévoit le droit interne du pays tiers.

49. Ces garanties requièrent un certain degré d'interprétation, en particulier du fait que la législation du pays tiers ne doit pas nécessairement être identique au cadre juridique de l'Union.

50. Comme l'a déclaré la CouEDH dans l'arrêt Kennedy, une «appréciation de cette question dépend de toutes les circonstances de la cause, par exemple la nature, l'étendue et la durée des mesures éventuelles, les raisons requises pour les ordonner, les autorités compétentes pour les permettre, exécuter et contrôler, le type de recours fourni par le droit interne»[71].

51. Par conséquent, l'appréciation des mesures de surveillance d'un pays tiers à l'aune des garanties essentielles européennes peut aboutir à deux conclusions:

[64] Article 13 de la CEDH.
[65] CouEDH, Klass, § 67.
[66] Schrems II, § 194.
[67] Schrems II, § 197, où la Cour utilise expressément ce terme.
[68] Schrems II, § 195.
[69] Schrems II, § 197, où la Cour utilise expressément ce terme.
[70] Schrems II, § 196.
[71] CouEDH, Kennedy, § 153.

- La réglementation du pays tiers concerné ne satisfait pas aux exigences des garanties essentielles européennes: dans ce cas, la réglementation du pays tiers n'offrirait pas un niveau de protection essentiellement équivalent à celui qui est garanti dans l'Union;

- La réglementation du pays tiers concerné satisfait aux exigences des garanties essentielles européennes.

52. Lors de l'appréciation du caractère adéquat du niveau de protection au titre de l'article 45 du RGPD, la Commission devra évaluer s'il est satisfait aux garanties essentielles européennes dans le cadre des éléments à prendre en considération pour garantir que la législation du pays tiers dans son ensemble offre un niveau de protection essentiellement équivalent à celui qui est garanti dans l'Union.

53. Lorsque des exportateurs – et des importateurs – de données s'appuient sur des garanties appropriées au titre de l'article 46 du RGPD, compte tenu des exigences de la législation du pays tiers spécifiquement applicable aux données transférées, ils devraient veiller à ce qu'un niveau de protection essentiellement équivalent soit effectivement atteint. En particulier, lorsque la législation du pays tiers ne respecte pas les exigences des garanties essentielles européennes, cela impliquerait de veiller à ce que cette législation n'empiète pas sur les garanties et mesures de protection relatives aux transferts, afin qu'un niveau de protection essentiellement équivalent à celui garanti dans l'Union soit maintenu.

54. Le comité européen de la protection des données a publié d'autres orientations et recommandations à prendre en considération pour procéder à cette évaluation, en fonction de l'outil de transfert utilisé et de la nécessité de prévoir des garanties appropriées, y compris, le cas échéant, des mesures supplémentaires[72].

55. Par ailleurs, il convient de relever que les garanties essentielles européennes sont basées sur des prescriptions légales. Le comité européen de la protection des données souligne que ces garanties reposent sur les droits fondamentaux qui s'appliquent à toute personne, quelle que soit sa nationalité.

56. Le comité européen de la protection des données rappelle que les garanties essentielles européennes constituent une norme de référence aux fins de l'évaluation de l'ingérence résultant des mesures de surveillance d'un pays tiers dans le cadre des transferts internationaux de données. Ces normes découlent du droit de l'Union et de la jurisprudence de la CJUE et de la CouEDH, qui est contraignante pour les États membres.

[72] Critères de référence pour l'adéquation WP 254 rev.01, version révisée et adoptée le 6 février 2018; recommandations du Comité européen de la protection des données 01/2020 relatives aux mesures complétant les outils de transfert afin de garantir le respect du niveau de protection des données à caractère personnel de l'UE, 10 novembre 2020.