



2023/2131

11.10.2023

RÈGLEMENT (UE) 2023/2131 DU PARLEMENT EUROPÉEN ET DU CONSEIL

du 4 octobre 2023

modifiant le règlement (UE) 2018/1727 du Parlement européen et du Conseil et la décision 2005/671/JAI du Conseil en ce qui concerne l'échange d'informations numériques dans les affaires de terrorisme

LE PARLEMENT EUROPÉEN ET LE CONSEIL DE L'UNION EUROPÉENNE,

vu le traité sur le fonctionnement de l'Union européenne, et notamment son article 85,

vu la proposition de la Commission européenne,

après transmission du projet d'acte législatif aux parlements nationaux,

statuant conformément à la procédure législative ordinaire ⁽¹⁾,

considérant ce qui suit:

- (1) Le règlement (UE) 2018/1727 du Parlement européen et du Conseil ⁽²⁾ a institué Eurojust et définit ses missions, ses compétences et ses fonctions.
- (2) La décision 2005/671/JAI du Conseil ⁽³⁾ dispose que, pour lutter contre le terrorisme, il est essentiel que les services concernés disposent des informations les plus complètes et les plus actualisées possibles. Cette décision impose aux autorités compétentes des États membres de communiquer à Eurojust des informations concernant les poursuites et les condamnations pour infractions terroristes qui intéressent ou sont susceptibles d'intéresser deux États membres ou plus.
- (3) En raison de divergences dans l'interprétation de la décision 2005/671/JAI, il arrive que, dans certains cas, les informations ne soient pas partagées en temps utile, qu'elles ne soient pas du tout partagées, ou que les informations pertinentes ne soient pas toutes partagées. Eurojust doit recevoir suffisamment d'informations pour être en mesure de détecter des liens entre les enquêtes transfrontières.
- (4) L'une des missions importantes d'Eurojust au titre du règlement (UE) 2018/1727 consiste à aider les autorités compétentes des États membres à garantir la meilleure coordination possible des enquêtes et des poursuites, y compris pour ce qui est de détecter des liens entre ces enquêtes et poursuites. Ledit règlement permet à Eurojust d'adopter une approche plus proactive et de fournir de meilleurs services aux États membres, par exemple en proposant l'ouverture d'enquêtes et en recensant les besoins de coordination, les cas qui violent potentiellement le principe ne bis in idem et les lacunes en matière de poursuites.
- (5) En septembre 2019, Eurojust a mis en place un registre judiciaire antiterroriste européen sur la base de la décision 2005/671/JAI, dans le but spécifique de détecter des liens potentiels entre les procédures judiciaires visant les personnes soupçonnées d'infractions terroristes et de déterminer les éventuels besoins de coordination découlant de tels liens.
- (6) Le registre judiciaire antiterroriste européen a été établi après l'adoption du règlement (UE) 2018/1727 et, par conséquent, ce registre n'est pas bien intégré dans l'infrastructure technique d'Eurojust ni visé dans le règlement (UE) 2018/1727. Il est donc nécessaire de remédier à cette situation.
- (7) Afin de lutter de manière effective contre le terrorisme, il est indispensable que les informations concernant des enquêtes ou des poursuites pour infractions terroristes soient échangées de manière efficace entre les autorités nationales compétentes et les agences de l'Union. Il est essentiel de disposer des informations les plus complètes et les plus actualisées possibles.

⁽¹⁾ Position du Parlement européen du 12 juillet 2023 (non encore parue au Journal officiel) et décision du Conseil du 18 septembre 2023.

⁽²⁾ Règlement (UE) 2018/1727 du Parlement européen et du Conseil du 14 novembre 2018 relatif à l'Agence de l'Union européenne pour la coopération judiciaire en matière pénale (Eurojust) et remplaçant et abrogeant la décision 2002/187/JAI du Conseil (JO L 295 du 21.11.2018, p. 138).

⁽³⁾ Décision 2005/671/JAI du Conseil du 20 septembre 2005 relative à l'échange d'informations et à la coopération concernant les infractions terroristes (JO L 253 du 29.9.2005, p. 22).

- (8) Les organisations terroristes sont de plus en plus impliquées dans d'autres formes graves de criminalité et font souvent partie de réseaux organisés. Une telle implication concerne des infractions graves telles que la traite d'êtres humains, le trafic de stupéfiants, la criminalité financière et le blanchiment d'argent. Il est nécessaire de recouper les procédures judiciaires engagées contre ces formes graves de criminalité.
- (9) Afin de permettre à Eurojust de détecter des liens entre les procédures judiciaires transfrontières visant des personnes soupçonnées d'infractions terroristes, ainsi que des liens entre les procédures judiciaires visant de telles personnes et les informations traitées au sein d'Eurojust concernant d'autres cas d'infractions graves, il est essentiel qu'Eurojust reçoive des autorités nationales compétentes, dès que possible et conformément aux dispositions pertinentes du présent règlement, les informations qui sont nécessaires pour permettre à Eurojust de détecter ces liens au moyen de recoupements.
- (10) En vue d'assurer la communication de données à Eurojust, les autorités nationales compétentes doivent savoir avec précision quel type d'informations il leur incombe de transmettre, à quel stade des procédures pénales nationales et dans quels cas. Les autorités nationales compétentes devraient transmettre les informations à Eurojust de manière structurée, organisée, systématique et semi-automatique. Une méthode semi-automatique est une méthode dans le cadre de laquelle le mode de transmission des informations est partiellement automatisé et partiellement sous contrôle humain. Cette méthode de transmission devrait accroître sensiblement la qualité et la pertinence des informations que reçoit Eurojust.
- (11) Le partage, le stockage et le recoupement des données accroîtront sensiblement la quantité de données traitées par Eurojust. Ces éléments devraient être pris en compte pour déterminer, dans le contexte des procédures et cadres existants, les ressources financières, humaines et techniques requises par Eurojust.
- (12) La directive (UE) 2017/541 du Parlement européen et du Conseil ^(*), telle qu'elle a été transposée en droit national, constitue le point de référence des autorités nationales compétentes pour la définition des infractions terroristes.
- (13) Il est essentiel d'échanger des données d'identification fiables afin de permettre à Eurojust de détecter des liens entre les enquêtes antiterroristes et les procédures judiciaires visant les personnes soupçonnées d'infractions terroristes. Il est également essentiel pour Eurojust de posséder et de stocker un ensemble de données qui permette d'identifier de manière fiable les personnes faisant l'objet de telles enquêtes ou procédures judiciaires en matière de terrorisme. L'utilisation de données biométriques est donc importante, compte tenu des incertitudes liées aux données alphanumériques, notamment en ce qui concerne les ressortissants de pays tiers, du fait que les suspects utilisent parfois de fausses ou doubles identités, et du fait que ces données biométriques sont souvent le seul lien avec les suspects au cours de la phase d'enquête. Par conséquent, lorsque, au titre du droit de la procédure pénale national ou du droit national en matière de droits procéduraux dans le cadre de procédures pénales, les autorités nationales compétentes stockent et recueillent des données biométriques et sont autorisées à les transmettre, ces autorités devraient être en mesure d'échanger ces données, lorsqu'elles en disposent, avec Eurojust. Compte tenu du caractère sensible des données biométriques et de l'incidence qu'a le traitement des données biométriques sur le respect de la vie privée et familiale et la protection des données à caractère personnel, consacrés aux articles 7 et 8 de la Charte des droits fondamentaux de l'Union européenne, ces données devraient être transmises d'une manière qui respecte strictement les principes de nécessité, de proportionnalité et de limitation de la finalité et dans le seul but d'identifier les personnes faisant l'objet de procédures pénales liées à des infractions terroristes.
- (14) Les informations concernant les liens existant avec d'autres procédures judiciaires étant surtout utiles aux premiers stades de l'enquête, il est nécessaire que les autorités nationales compétentes fournissent les informations à Eurojust dès qu'une autorité judiciaire est saisie d'une affaire conformément au droit national. Une autorité judiciaire devrait être réputée saisie d'une affaire lorsque, par exemple, elle est informée d'une enquête en cours, elle approuve ou ordonne une mesure d'enquête, ou elle décide des poursuites, en fonction du droit national applicable. Si une autorité nationale compétente a déjà connaissance de liens entre une procédure pénale dans son État membre et une procédure pénale dans un autre État membre, elle devrait en aviser Eurojust.

^(*) Directive (UE) 2017/541 du Parlement européen et du Conseil du 15 mars 2017 relative à la lutte contre le terrorisme et remplaçant la décision-cadre 2002/475/JAI du Conseil et modifiant la décision 2005/671/JAI du Conseil (JO L 88 du 31.3.2017, p. 6).

- (15) Compte tenu du fait que, dans les systèmes et traditions juridiques de certains États membres, une autorité judiciaire ne supervise pas les enquêtes et n'intervient qu'à des stades ultérieurs de la procédure, le présent règlement ne devrait pas empêcher les autorités nationales compétentes de communiquer des informations sur les enquêtes en matière de terrorisme à leurs membres nationaux à un stade plus précoce, conformément à leur droit national.
- (16) Afin de garantir l'exactitude des données inscrites dans le registre judiciaire antiterroriste européen, de détecter des liens ou de déterminer l'identité d'un suspect le plus tôt possible au cours d'une enquête et de veiller au respect des délais, les autorités nationales compétentes devraient actualiser les informations qu'elles ont communiquées. Ces actualisations devraient inclure de nouvelles informations relatives à la personne faisant l'objet de l'enquête, aux décisions judiciaires telles que la détention préventive, l'ouverture de procédures juridictionnelles, les acquittements et les décisions définitives de ne pas engager de poursuites, ainsi qu'aux demandes de coopération judiciaire ou aux liens recensés avec d'autres juridictions.
- (17) Les autorités nationales compétentes ne devraient pas être tenues de partager des informations concernant des infractions terroristes avec Eurojust dès le stade initial de la procédure lorsque cela risque de compromettre les enquêtes en cours ou la sécurité d'une personne ou si cela est contraire aux intérêts essentiels de la sécurité de l'État membre concerné. Ces dérogations à l'obligation de partager des informations ne devraient s'appliquer que dans des circonstances exceptionnelles et au cas par cas. En vue de déterminer s'il convient ou non de déroger à cette obligation, les autorités nationales compétentes devraient tenir dûment compte du fait qu'Eurojust traite les informations qu'elles lui fournissent conformément au droit de l'Union en matière de protection des données, et de la confidentialité des procédures judiciaires.
- (18) Aux fins de l'échange des données sensibles entre les autorités nationales compétentes et Eurojust et du traitement de ces données, il convient d'utiliser des canaux de communication sécurisés, tels qu'un système informatique décentralisé ou l'accès à des télécommunications sécurisées visé dans la décision 2008/976/JAI du Conseil ⁽⁵⁾, afin de protéger ces données contre toute divulgation non autorisée et contre les cyberattaques. Une telle utilisation devrait s'entendre sans préjudice des évolutions technologiques futures.
- (19) Afin d'échanger les données de manière sécurisée et de protéger l'intégrité de la communication et de l'échange de données, le système de gestion des dossiers devrait être connecté à des canaux de communication sécurisés et répondre à des normes élevées en matière de cybersécurité. Ces canaux de communication sécurisés peuvent également être utilisés pour connecter le système de gestion des dossiers à d'autres systèmes d'information de l'Union, dans la mesure où les actes juridiques établissant ces systèmes prévoient un accès par Eurojust.
- (20) Le système informatique décentralisé devrait permettre des échanges de données sécurisés entre les autorités nationales compétentes et Eurojust, sans qu'aucune institution ou aucun organe ou organisme de l'Union n'intervienne dans le contenu de ces échanges. Le système informatique décentralisé devrait comprendre les systèmes dorsaux informatiques des États membres et d'Eurojust qui sont interconnectés par des points d'accès interopérables. Les points d'accès du système informatique décentralisé devraient être basés sur e-CODEX.
- (21) Afin d'assurer des conditions uniformes d'exécution du présent règlement en ce qui concerne l'établissement et l'utilisation du système informatique décentralisé pour les affaires couvertes par le présent règlement, il convient de conférer des compétences d'exécution à la Commission. Ces compétences devraient être exercées conformément au règlement (UE) n° 182/2011 du Parlement européen et du Conseil ⁽⁶⁾.
- (22) La transmission de données non structurées rend l'intervention manuelle nécessaire, crée une charge administrative supplémentaire et affecte la qualité des résultats du recoupement. Par conséquent, les autorités nationales compétentes devraient transmettre les données de manière structurée tout en respectant les exigences minimales en matière d'interopérabilité définies dans le cadre d'interopérabilité européen visé dans la communication de la Commission du 23 mars 2017 intitulée «Cadre d'interopérabilité européen – Stratégie de mise en œuvre». En outre, le transfert des données devrait être automatisé autant que possible afin de réduire la charge administrative pesant sur les autorités nationales compétentes et d'assurer une transmission régulière et rapide des données nécessaires.

⁽⁵⁾ Décision 2008/976/JAI du Conseil du 16 décembre 2008 concernant le Réseau judiciaire européen (JO L 348 du 24.12.2008, p. 130).

⁽⁶⁾ Règlement (UE) n° 182/2011 du Parlement européen et du Conseil du 16 février 2011 établissant les règles et principes généraux relatifs aux modalités de contrôle par les États membres de l'exercice des compétences d'exécution par la Commission (JO L 55 du 28.2.2011, p. 13).

- (23) La modernisation du système de gestion des dossiers est nécessaire pour permettre à Eurojust de traiter les données à caractère personnel sensibles de manière sécurisée. Le nouveau système doit intégrer et rendre possibles les fonctionnalités du registre judiciaire antiterroriste européen et améliorer la capacité d'Eurojust à détecter des liens, tout en tirant pleinement parti, en règle générale, des mécanismes nationaux et de l'Union existants en matière de comparaison des données biométriques.
- (24) Il importe de maintenir le contrôle et la responsabilité incombant aux membres nationaux en ce qui concerne les données qu'ils reçoivent de la part des autorités nationales compétentes. Aucune donnée opérationnelle à caractère personnel ne devrait être partagée par défaut avec un autre État membre. Les données opérationnelles à caractère personnel ne devraient être partagées que dans la mesure où les autorités nationales compétentes autorisent l'échange de données. Pour numériser et accélérer le suivi des liens potentiels, tout en assurant un contrôle total des données, des codes de traitement devraient être introduits.
- (25) Aujourd'hui, le terrorisme et la grande criminalité organisée sont des phénomènes mondialisés et en évolution constante, qui touchent souvent deux États membres ou plus. Bien que le terrorisme ait déjà une forte composante transnationale, du fait de l'utilisation et de la disponibilité des communications électroniques, la collaboration transnationale entre les auteurs d'infractions terroristes s'est sensiblement accrue. Le caractère transnational d'une infraction terroriste peut ne pas être connu lorsqu'une autorité judiciaire est saisie de l'affaire, mais il pourrait être révélé lors du recoupement des données par Eurojust. Les enquêtes ou les poursuites concernant des infractions terroristes nécessitent donc une coordination et une coopération entre les autorités chargées des poursuites ou une poursuite sur des bases communes, comme le prévoit l'article 85 du traité sur le fonctionnement de l'Union européenne. Les informations relatives aux affaires de terrorisme devraient être échangées avec Eurojust en temps utile, à moins que les circonstances particulières de l'affaire n'indiquent clairement que celle-ci a un caractère purement national.
- (26) Dans les affaires de terrorisme, les enquêtes et les poursuites sont souvent entravées par le manque d'échange d'informations entre les autorités nationales chargées des enquêtes et des poursuites. Afin d'être en mesure de recouper les nouvelles enquêtes en matière de terrorisme avec les anciennes enquêtes et de détecter des liens potentiels, il est nécessaire de veiller à ce que la durée de conservation des données relatives à toute enquête et condamnation antérieure soit suffisante pour les activités opérationnelles. Il est donc nécessaire de prolonger les délais applicables à la conservation des données dans le registre judiciaire antiterroriste européen.
- (27) La possibilité de recouper les nouvelles enquêtes en matière de terrorisme avec d'anciennes enquêtes pourrait permettre de détecter des liens potentiels et engendrer la nécessité d'une coopération. Un tel recoupement pourrait révéler qu'une personne soupçonnée ou poursuivie dans une affaire en cours dans un État membre a été soupçonnée ou poursuivie dans une affaire close dans un autre État membre. Il pourrait également permettre de détecter des liens entre des enquêtes ou des poursuites en cours qui auraient pu, sans cela, rester cachés. C'est le cas même lorsque des enquêtes antérieures ont abouti à un acquittement ou à une décision définitive de ne pas engager de poursuites. Il est donc nécessaire de conserver les données relatives à toute enquête antérieure, en tant que de besoin, et pas seulement celles relatives aux condamnations.
- (28) Il est nécessaire de veiller à ce que les données issues d'enquêtes qui ont abouti à un acquittement ou à une décision définitive de ne pas engager de poursuites ne soient traitées qu'à des fins de poursuites. Ces données ne peuvent être utilisées à des fins autres que la détection de liens avec des enquêtes et poursuites en cours et le soutien de ces enquêtes et poursuites. Sauf si l'autorité nationale compétente en décide autrement au cas par cas, Eurojust devrait pouvoir continuer à traiter ces données opérationnelles. Lorsque, après que la décision d'acquiescement ou de ne pas engager de poursuites est devenue définitive, l'autorité nationale compétente décide que le traitement des données des personnes acquittées ou ne faisant pas l'objet de poursuites n'est pas nécessaire, notamment en raison des spécificités de l'affaire ou des motifs de l'acquiescement ou de l'absence de poursuites, ces données devraient être effacées.
- (29) Eurojust a conclu douze accords de coopération avec des pays tiers, qui autorisent le transfert de données opérationnelles à caractère personnel ainsi que le détachement auprès d'Eurojust de procureurs de liaison de pays tiers. En outre, l'accord de commerce et de coopération entre l'Union européenne et la Communauté européenne de l'énergie atomique, d'une part, et le Royaume-Uni de Grande-Bretagne et d'Irlande du Nord, d'autre part ⁽⁷⁾, autorise le détachement d'un procureur de liaison. En mars 2021, le Conseil a mandaté la Commission pour négocier des accords de coopération entre Eurojust et treize autres pays tiers, à savoir l'Algérie, l'Argentine, l'Arménie, la Bosnie-Herzégovine, le Brésil, la Colombie, l'Égypte, Israël, la Jordanie, le Liban, le Maroc, la Tunisie et la Turquie.

(7) JO L 149 du 30.4.2021, p. 10.

- (30) Bien que le règlement (UE) 2018/1727 constitue la base juridique de la coopération et de l'échange de données avec les pays tiers, il ne comporte aucune règle sur les aspects formels et techniques de la coopération avec les procureurs de liaison de pays tiers détachés auprès d'Eurojust, notamment en ce qui concerne leur accès au système de gestion des dossiers. Dans un souci de sécurité juridique, le règlement (UE) 2018/1727 devrait fournir une base juridique explicite pour la coopération entre Eurojust et les procureurs de liaison de pays tiers et leur accès au système de gestion des dossiers. Eurojust devrait appliquer des garanties et des mesures de sécurité appropriées aux fins de la protection des données et des droits fondamentaux grâce à une configuration technique mise à jour et à des règles internes strictes.
- (31) Lorsqu'elle traite des données opérationnelles à caractère personnel conformément au présent règlement, Eurojust devrait assurer un niveau élevé de protection des données. Pour le traitement des données opérationnelles à caractère personnel, Eurojust est soumise à l'article 3 et au chapitre IX du règlement (UE) 2018/1725 du Parlement européen et du Conseil ⁽⁸⁾, ainsi qu'aux règles spécifiques relatives au traitement des données opérationnelles à caractère personnel prévues par le règlement (UE) 2018/1727 tel qu'il a été modifié par le règlement (UE) 2022/838 du Parlement européen et du Conseil ⁽⁹⁾ et par le présent règlement. Ces dispositions s'appliquent au traitement de toutes les données opérationnelles à caractère personnel traitées par Eurojust. En particulier, elles s'appliquent à toutes les données opérationnelles à caractère personnel traitées dans le système de gestion des dossiers, qu'elles soient traitées par des membres nationaux, des correspondants nationaux, des procureurs de liaison ou d'autres personnes autorisées conformément au règlement (UE) 2018/1727.
- (32) Les décisions sur la question de savoir si et comment Eurojust devrait soutenir la coordination et la coopération entre les autorités chargées des enquêtes et des poursuites devraient rester du ressort exclusif des autorités compétentes des États membres concernés, sous réserve du droit national applicable, du droit de l'Union ou du droit international, comprenant des conventions ou d'autres accords internationaux relatifs à l'entraide judiciaire en matière pénale.
- (33) Dans un souci de sécurité juridique, il y a lieu de clarifier la relation entre l'échange d'informations intervenant entre les autorités nationales compétentes dans les affaires de terrorisme et Eurojust dans le cadre de la décision 2005/671/JAI et du règlement (UE) 2018/1727. Par conséquent, les dispositions concernées devraient être supprimées dans la décision 2005/671/JAI et devraient être ajoutées au règlement (UE) 2018/1727.
- (34) Si certaines autorités nationales compétentes disposent déjà de l'accès aux télécommunications sécurisées visé à l'article 9 de la décision 2008/976/JAI, de nombreuses autorités nationales compétentes ne disposent pas encore de cet accès aux télécommunications sécurisées ou à des canaux de communication sécurisés. Afin de s'assurer que les États membres disposent de suffisamment de temps pour offrir un tel accès aux autorités nationales compétentes, une période transitoire devrait être octroyée en vue de sa mise en œuvre.
- (35) Conformément aux articles 1^{er} et 2 ainsi qu'à l'article 4 bis, paragraphe 1, du protocole n° 21 sur la position du Royaume-Uni et de l'Irlande à l'égard de l'espace de liberté, de sécurité et de justice, annexé au traité sur l'Union européenne et au traité sur le fonctionnement de l'Union européenne, et sans préjudice de l'article 4 dudit protocole, l'Irlande ne participe pas à l'adoption du présent règlement et n'est pas liée par celui-ci ni soumise à son application.
- (36) Conformément aux articles 1^{er} et 2 du protocole n° 22 sur la position du Danemark annexé au traité sur l'Union européenne et au traité sur le fonctionnement de l'Union européenne, le Danemark ne participe pas à l'adoption du présent règlement et n'est pas lié par celui-ci ni soumis à son application.
- (37) Le Contrôleur européen de la protection des données a été consulté conformément à l'article 42 du règlement (UE) 2018/1725 et a rendu un avis le 26 janvier 2022,

⁽⁸⁾ Règlement (UE) 2018/1725 du Parlement européen et du Conseil du 23 octobre 2018 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions, organes et organismes de l'Union et à la libre circulation de ces données, et abrogeant le règlement (CE) n° 45/2001 et la décision n° 1247/2002/CE (JO L 295 du 21.11.2018, p. 39).

⁽⁹⁾ Règlement (UE) 2022/838 du Parlement européen et du Conseil du 30 mai 2022 modifiant le règlement (UE) 2018/1727 en ce qui concerne la préservation, l'analyse et la conservation, au sein d'Eurojust, des éléments de preuve relatifs aux génocides, aux crimes contre l'humanité, aux crimes de guerre et aux infractions pénales connexes (JO L 148 du 31.5.2022, p. 1).

ONT ADOPTÉ LE PRÉSENT RÈGLEMENT:

Article premier

Modifications du règlement (UE) 2018/1727

Le règlement (UE) 2018/1727 est modifié comme suit:

1) À l'article 3, le paragraphe 5 est remplacé par le texte suivant:

«5. Eurojust peut également apporter son assistance dans les enquêtes et les poursuites qui ne concernent qu'un État membre et un pays tiers, ou un État membre et une organisation internationale, à condition qu'un accord de coopération ou un arrangement instaurant une coopération en vertu de l'article 52 ait été conclu avec ce pays tiers ou cette organisation internationale ou que, dans un cas particulier, il y ait un intérêt essentiel à apporter une telle assistance.

La décision relative à la question de savoir si et de quelle manière les États membres apportent une assistance judiciaire à un pays tiers ou à une organisation internationale continue de relever exclusivement de l'autorité compétente de l'État membre concerné, sous réserve du droit national applicable, du droit de l'Union ou du droit international.»

2) L'article 20 est modifié comme suit:

a) le paragraphe suivant est inséré:

«2 bis. Chaque État membre désigne une autorité nationale compétente en tant que correspondant national pour Eurojust pour les questions de terrorisme. Ce correspondant national pour les questions de terrorisme est une autorité judiciaire ou une autre autorité compétente. Lorsque l'ordre juridique national l'exige, un État membre doit pouvoir désigner plusieurs autorités nationales compétentes en tant que correspondant national pour Eurojust pour les questions de terrorisme. Le correspondant national pour les questions de terrorisme a accès à toutes les informations pertinentes conformément à l'article 21 bis, paragraphe 1. Il est compétent pour recueillir ces informations et les transmettre à Eurojust, conformément au droit national et au droit de l'Union, en particulier le droit de la procédure pénale national et les règles applicables en matière de protection des données.»;

b) le paragraphe 8 est remplacé par le texte suivant:

«8. Aux fins de la réalisation des objectifs visés au paragraphe 7 du présent article, les personnes visées au paragraphe 3, points a), b) et c), du présent article sont connectées au système de gestion des dossiers conformément au présent article et aux articles 23, 24, 25 et 34. Le coût de la connexion au système de gestion des dossiers est à la charge du budget général de l'Union.».

3) L'article 21 est modifié comme suit:

a) le paragraphe 9 est remplacé par le texte suivant:

«9. Le présent article est sans incidence sur d'autres obligations relatives à la transmission d'informations à Eurojust.»;

b) le paragraphe 10 est remplacé par le texte suivant:

«10. Les autorités nationales compétentes ne sont pas tenues de fournir les informations visées au présent article lorsque ces informations ont déjà été transmises à Eurojust conformément à d'autres dispositions du présent règlement.».

4) L'article suivant est inséré:

«Article 21 bis

Échange d'informations relatives aux affaires de terrorisme

1. En ce qui concerne les infractions terroristes, les autorités nationales compétentes informent leurs membres nationaux de toute enquête pénale en cours ou close supervisée par les autorités judiciaires dès que celles-ci sont saisies de l'affaire conformément au droit national, en particulier le droit de la procédure pénale national, de toutes

poursuites ou procédures judiciaires en cours ou closes et de toutes décisions judiciaires, concernant des infractions terroristes. Cette obligation s'applique à toutes les enquêtes pénales relatives à des infractions terroristes, qu'il existe ou non un lien connu avec un autre État membre ou un pays tiers, à moins que l'enquête pénale, en raison des circonstances particulières qui s'y rapportent, ne concerne manifestement qu'un seul État membre.

2. Le paragraphe 1 ne s'applique pas lorsque:

- a) le partage d'informations compromettrait une enquête en cours ou la sécurité d'une personne; ou
- b) le partage d'informations serait contraire aux intérêts essentiels de l'État membre concerné en matière de sécurité.

3. Les infractions terroristes aux fins du présent article sont les infractions visées dans la directive (UE) 2017/541 du Parlement européen et du Conseil (*).

4. Les informations transmises conformément au paragraphe 1 comprennent les données opérationnelles à caractère personnel et les données à caractère non personnel figurant à l'annexe III. Ces informations peuvent comprendre des données à caractère personnel conformément à l'annexe III, point d), mais seulement si ces données à caractère personnel sont détenues par les autorités nationales compétentes ou peuvent être communiquées à celles-ci conformément au droit national et si la transmission de ces données est nécessaire pour identifier de manière fiable une personne concernée au titre de l'article 27, paragraphe 5.

5. Sous réserve du paragraphe 2, les autorités nationales compétentes informent leurs membres nationaux de toute modification apportée aux informations transmises au titre du paragraphe 1 sans retard injustifié et, dans la mesure du possible, au plus tard dix jours ouvrables après ladite modification.

6. L'autorité nationale compétente n'est pas tenue de fournir ces informations lorsqu'elles ont déjà été transmises à Eurojust.

7. L'autorité nationale compétente peut, à tout moment, demander le soutien d'Eurojust dans le cadre des mesures de suivi concernant les liens détectés sur la base des informations fournies au titre du présent article.

(*) Directive (UE) 2017/541 du Parlement européen et du Conseil du 15 mars 2017 relative à la lutte contre le terrorisme et remplaçant la décision-cadre 2002/475/JAI du Conseil et modifiant la décision 2005/671/JAI du Conseil (JO L 88 du 31.3.2017, p. 6).

5) Les articles suivants sont insérés:

«Article 22 bis

Communication numérique et échange d'informations sécurisés entre les autorités nationales compétentes et Eurojust

1. La communication entre les autorités nationales compétentes et Eurojust au titre du présent règlement s'effectue au moyen d'un système informatique décentralisé. Le système de gestion des dossiers visé à l'article 23 est connecté à un réseau de systèmes informatiques et de points d'accès e-CODEX interopérables, dont le fonctionnement relève de la responsabilité et de la gestion individuelles de chaque État membre et d'Eurojust, permettant un échange d'informations transfrontière sécurisé et fiable (ci-après dénommé «système informatique décentralisé»).

2. Lorsque l'échange d'informations, conformément au paragraphe 1, se révèle impossible en raison de l'indisponibilité du système informatique décentralisé ou en raison de circonstances exceptionnelles, ledit échange est effectué à l'aide des moyens de substitution les plus rapides et les plus appropriés. Les États membres et Eurojust veillent à ce que les moyens de communication de substitution soient fiables et offrent un niveau de sécurité et de protection des données équivalent.

3. Les autorités nationales compétentes transmettent les informations visées aux articles 21 et 21 bis du présent règlement à Eurojust de manière semi-automatisée et structurée, à partir des registres nationaux. Les modalités de cette transmission sont déterminées par la Commission, après consultation d'Eurojust, dans un acte d'exécution, conformément à l'article 22 ter du présent règlement. En particulier, ledit acte d'exécution détermine le format des données transmises en vertu de l'annexe III, point d), du présent règlement et les normes techniques nécessaires en ce qui concerne la transmission de ces données, et définit les normes de procédure numériques telles qu'elles sont définies à l'article 3, point 9), du règlement (UE) 2022/850 du Parlement européen et du Conseil (*).

4. La Commission est responsable de la création, de la maintenance et du développement d'un logiciel de mise en œuvre de référence que les États membres et Eurojust peuvent choisir d'utiliser comme système dorsal. Ce logiciel de mise en œuvre de référence est basé sur une configuration modulaire, ce qui signifie que le logiciel est conditionné et livré séparément des composants e-CODEX nécessaires pour le connecter au système informatique décentralisé. Cette configuration permet aux États membres de réutiliser ou d'améliorer leurs infrastructures nationales de communication judiciaire existantes à des fins d'utilisation transfrontière et permet à Eurojust de connecter son système de gestion des dossiers au système informatique décentralisé.

5. La Commission assure à titre gratuit la fourniture et la maintenance du logiciel de mise en œuvre de référence ainsi que l'assistance y afférente. La création, la maintenance et le développement du logiciel de mise en œuvre de référence sont financés par le budget général de l'Union.

6. Les États membres et Eurojust prennent en charge les coûts qui leur incombent respectivement pour l'établissement et l'exploitation d'un point d'accès e-CODEX autorisé tel qu'il est défini à l'article 3, point 3), du règlement (UE) 2022/850, et pour l'établissement et l'adaptation de leurs systèmes informatiques concernés afin de les rendre interopérables avec les points d'accès.

Article 22 ter

Adoption d'actes d'exécution par la Commission

1. La Commission adopte les actes d'exécution nécessaires à l'établissement et à l'utilisation du système informatique décentralisé pour la communication au titre du présent règlement, ces actes précisant les éléments suivants:

- a) les spécifications techniques définissant les méthodes de communication par voie électronique aux fins du système informatique décentralisé;
- b) les spécifications techniques concernant les protocoles de communication;
- c) les objectifs en matière de sécurité de l'information et les mesures techniques pertinentes garantissant des normes minimales de sécurité de l'information ainsi que des normes élevées en matière de cybersécurité pour le traitement et la communication des informations au sein du système informatique décentralisé;
- d) les objectifs minimaux en matière de disponibilité et les éventuelles exigences techniques correspondantes pour les services fournis par le système informatique décentralisé;
- e) la création d'un comité directeur composé de représentants des États membres, chargé d'assurer le fonctionnement et la maintenance du système informatique décentralisé afin d'atteindre les objectifs du présent règlement.

2. Les actes d'exécution visés au paragraphe 1 du présent article sont adoptés au plus tard le 1^{er} novembre 2025 conformément à la procédure d'examen visée à l'article 22 quater, paragraphe 2.

Article 22 quater

Comité

1. La Commission est assistée par un comité. Ledit comité est un comité au sens du règlement (UE) n° 182/2011 du Parlement européen et du Conseil (**).

2. Lorsqu'il est fait référence au présent paragraphe, l'article 5 du règlement (UE) n° 182/2011 s'applique.

Lorsque le comité n'émet aucun avis, la Commission n'adopte pas le projet d'acte d'exécution, et l'article 5, paragraphe 4, troisième alinéa, du règlement (UE) n° 182/2011 s'applique.

- (*) Règlement (UE) 2022/850 du Parlement européen et du Conseil du 30 mai 2022 relatif à un système informatisé pour l'échange électronique transfrontière de données dans le domaine de la coopération judiciaire en matière civile et pénale (système e-CODEX), et modifiant le règlement (UE) 2018/1726 (JO L 150 du 1.6.2022, p. 1).
- (**) Règlement (UE) n° 182/2011 du Parlement européen et du Conseil du 16 février 2011 établissant les règles et principes généraux relatifs aux modalités de contrôle par les États membres de l'exercice des compétences d'exécution par la Commission (JO L 55 du 28.2.2011, p. 13).

- 6) Les articles 23, 24 et 25 sont remplacés par le texte suivant:

«Article 23

Système de gestion des dossiers

1. Eurojust établit un système de gestion des dossiers aux fins du traitement des données opérationnelles à caractère personnel énumérées à l'annexe II, des données énumérées à l'annexe III et des données à caractère non personnel.

2. Le système de gestion des dossiers a pour objectifs de:

- a) fournir un soutien à la conduite et à la coordination des enquêtes et des poursuites pour lesquelles Eurojust apporte une assistance;
- b) garantir un accès sécurisé aux informations relatives aux enquêtes et aux poursuites en cours, ainsi que l'échange de ces informations;
- c) permettre le recoupement d'informations et la détection de liens;
- d) permettre l'extraction de données à des fins opérationnelles et statistiques;
- e) faciliter le contrôle en vue de s'assurer que le traitement des données opérationnelles à caractère personnel est licite et respecte le présent règlement ainsi que les règles applicables en matière de protection des données.

3. Le système de gestion des dossiers peut être relié à l'accès aux télécommunications sécurisées visé à l'article 9 de la décision 2008/976/JAI du Conseil (*) et aux autres canaux de communication sécurisés conformément au droit applicable de l'Union.

4. Lorsqu'elle se voit accorder l'accès à des données figurant dans d'autres systèmes d'information de l'Union établis en vertu d'autres actes juridiques de l'Union ou provenant de tels systèmes d'information, Eurojust peut utiliser le système de gestion des dossiers pour avoir accès à des données figurant dans ces systèmes d'information ou pour se connecter à ces systèmes d'information aux fins d'extraire et de traiter des informations, y compris des données à caractère personnel, à condition que cela soit nécessaire à l'exécution de ses tâches et conforme aux actes juridiques de l'Union établissant ces systèmes d'information.

5. Les paragraphes 3 et 4 n'étendent pas les droits d'accès accordés à Eurojust à d'autres systèmes d'information de l'Union en vertu des actes juridiques de l'Union établissant ces systèmes.

6. Dans l'exercice de leurs fonctions, les membres nationaux peuvent traiter des données à caractère personnel relatives aux dossiers individuels sur lesquels ils travaillent, conformément au présent règlement ou à d'autres instruments applicables. Ils autorisent le délégué à la protection des données à avoir accès aux données à caractère personnel traitées dans le cadre du système de gestion des dossiers.

7. Pour traiter des données opérationnelles à caractère personnel, Eurojust ne crée pas de fichiers automatisés autres que ceux qui sont établis dans le cadre du système de gestion des dossiers.

Les membres nationaux peuvent stocker temporairement des données à caractère personnel et les analyser afin de déterminer si de telles données sont utiles à l'accomplissement des missions d'Eurojust et si elles peuvent être incluses dans le système de gestion des dossiers. Ces données peuvent être conservées pendant une durée maximale de trois mois.

Article 24

Gestion des informations dans le cadre du système de gestion des dossiers

1. Le membre national stocke les informations qui lui sont transmises dans le système de gestion des dossiers, conformément au présent règlement ou aux autres instruments applicables.

Le membre national est responsable de la gestion des données qu'il traite.

2. Le membre national décide, au cas par cas, de restreindre l'accès aux informations ou d'en accorder l'accès, intégral ou partiel, à d'autres membres nationaux, aux procureurs de liaison détachés auprès d'Eurojust, à des membres du personnel autorisés d'Eurojust ou à toute autre personne travaillant au nom d'Eurojust qui a reçu l'autorisation nécessaire du directeur administratif.

3. Le membre national indique, après consultation des autorités nationales compétentes, en termes généraux ou spécifiques, toutes restrictions concernant le traitement ultérieur et le transfert des informations, ou l'accès à celles-ci, si un lien, tel qu'il est visé à l'article 23, paragraphe 2, point c), a été détecté.

Article 25

Accès au système de gestion des dossiers au niveau national

1. Les personnes visées à l'article 20, paragraphe 3, points a), b) et c), n'ont accès qu'aux données suivantes:

- a) les données contrôlées par le membre national de leur État membre;
- b) les données contrôlées par les membres nationaux d'autres États membres et auxquelles le membre national de leur État membre a été autorisé à accéder, à moins que le membre national qui contrôle les données n'ait refusé cet accès.

2. Le membre national décide, dans les limites prévues au paragraphe 1 du présent article, de l'étendue de l'accès qui est accordé aux personnes visées à l'article 20, paragraphe 3, points a), b) et c), dans leur État membre.

3. Seuls les correspondants nationaux pour Eurojust pour les questions de terrorisme visés à l'article 20, paragraphe 3, point c), peuvent accéder au niveau national aux données fournies conformément à l'article 21 *bis*.

4. Chaque État membre peut décider, après consultation de son membre national, que les personnes visées à l'article 20, paragraphe 3, points a), b) et c), peuvent, dans les limites prévues aux paragraphes 1, 2 et 3 du présent article, introduire dans le système de gestion des dossiers des informations concernant leur État membre. Cette contribution est soumise à la validation du membre national concerné. Le collège détermine les modalités de la mise en œuvre pratique du présent paragraphe. Les États membres notifient à Eurojust et à la Commission leur décision en ce qui concerne la mise en œuvre du présent paragraphe. La Commission en informe les autres États membres.

(*) Décision 2008/976/JAI du Conseil du 16 décembre 2008 concernant le Réseau judiciaire européen (JO L 348 du 24.12.2008, p. 130).».

7) L'article 27 est modifié comme suit:

a) le paragraphe 4 est remplacé par le texte suivant:

«4. Eurojust peut traiter des catégories particulières de données opérationnelles à caractère personnel conformément à l'article 76 du règlement (UE) 2018/1725. Lorsque ces autres données concernent des témoins ou des victimes au sens du paragraphe 2 du présent article, la décision de les traiter est prise par les membres nationaux concernés.»;

b) le paragraphe suivant est ajouté:

«5. Lorsque des données opérationnelles à caractère personnel sont transmises conformément à l'article 21 *bis*, Eurojust peut traiter les données opérationnelles à caractère personnel énumérées à l'annexe III des personnes suivantes:

a) les personnes à l'égard desquelles, conformément au droit national de l'État membre concerné, il existe des motifs sérieux de croire qu'elles ont commis ou sont sur le point de commettre une infraction pénale pour laquelle Eurojust est compétente;

b) les personnes qui ont été condamnées pour une telle infraction.

Sauf si l'autorité nationale compétente en décide autrement au cas par cas, Eurojust peut poursuivre le traitement des données opérationnelles à caractère personnel mentionnées au premier alinéa, point a), y compris après la clôture des procédures en vertu du droit national de l'État membre concerné, même en cas d'acquiescement ou de décision définitive de ne pas engager de poursuites. Lorsque les procédures n'ont pas abouti à une condamnation, il n'est procédé au traitement des données opérationnelles à caractère personnel qu'aux fins de détecter des liens entre des enquêtes et des poursuites en cours, à venir ou closes, conformément à l'article 23, paragraphe 2, point c).».

8) L'article 29 est modifié comme suit:

a) le paragraphe suivant est inséré:

«1 *bis*. Eurojust ne peut conserver les données opérationnelles à caractère personnel transmises conformément à l'article 21 *bis* au-delà de la première des dates suivantes:

a) la date d'expiration du délai de prescription de l'action publique dans tous les États membres concernés par l'enquête ou les poursuites;

b) cinq ans après la date à laquelle est devenue définitive la décision judiciaire du dernier des États membres concernés par l'enquête ou les poursuites, ou deux ans en cas d'acquiescement ou de décision définitive de ne pas engager de poursuites;

c) la date à laquelle Eurojust est informée de la décision de l'autorité nationale compétente en vertu de l'article 27, paragraphe 5.»;

b) les paragraphes 2 et 3 sont remplacés par le texte suivant:

«2. Le respect des délais de conservation visés aux paragraphes 1 et 1 *bis* est vérifié de manière permanente par un traitement automatisé adéquat effectué par Eurojust, en particulier à partir du moment où Eurojust cesse de fournir une assistance.

Une vérification de la nécessité de conserver les données est également faite tous les trois ans après leur introduction.

Si des données opérationnelles à caractère personnel visées à l'article 27, paragraphe 4, sont conservées pendant une durée supérieure à cinq ans, le CEPD en est informé.

3. Avant que l'un des délais de conservation visés aux paragraphes 1 et 1 *bis* n'expire, Eurojust vérifie la nécessité de continuer à conserver les données opérationnelles à caractère personnel lorsque et aussi longtemps que cela est nécessaire à l'accomplissement de ses missions.

Elle peut décider de conserver ces données à titre dérogatoire jusqu'à la vérification suivante. Les raisons de prolonger la conservation des données sont justifiées et consignées. Si, au moment de la vérification, il n'est pas décidé de conserver plus longtemps les données opérationnelles à caractère personnel, celles-ci sont effacées automatiquement.».

9) L'article suivant est inséré:

«Article 54 bis

Procureurs de liaison de pays tiers

1. Un procureur de liaison provenant d'un pays tiers peut être détaché auprès d'Eurojust sur la base d'un accord de coopération conclu avant le 12 décembre 2019 entre Eurojust et le pays tiers en question, ou sur la base d'un accord international conclu entre l'Union et le pays tiers en vertu de l'article 218 du traité sur le fonctionnement de l'Union européenne, autorisant le détachement d'un procureur de liaison.

2. Les droits et obligations du procureur de liaison sont énoncés dans l'accord de coopération ou l'accord international visés au paragraphe 1 ou dans un arrangement de travail conclu conformément à l'article 47, paragraphe 3.

3. Les procureurs de liaison détachés auprès d'Eurojust obtiennent un accès au système de gestion des dossiers aux fins de l'échange sécurisé de données. Conformément aux articles 45 et 46, Eurojust reste responsable du traitement des données à caractère personnel effectué par les procureurs de liaison dans le cadre du système de gestion des dossiers.

Les transferts de données opérationnelles à caractère personnel effectués à l'aide du système de gestion des dossiers vers les procureurs de liaison de pays tiers ne peuvent avoir lieu que selon les règles et les conditions énoncées dans le présent règlement, dans l'accord conclu avec le pays concerné ou dans tout autre instrument juridique applicable.

L'article 24, paragraphe 1, deuxième alinéa, et l'article 24, paragraphe 2, s'appliquent mutatis mutandis aux procureurs de liaison.

Le collège établit les conditions précises d'accès.».

10) À l'article 80, les paragraphes suivants sont ajoutés:

«9. Eurojust peut continuer à utiliser le système de gestion des dossiers composé de fichiers de travail temporaires et d'un index jusqu'au 1^{er} décembre 2025, si le nouveau système de gestion des dossiers n'est pas encore en place.

10. Les autorités nationales compétentes et Eurojust peuvent continuer à utiliser des canaux de communication autres que ceux visés à l'article 22 bis, paragraphe 1, jusqu'au premier jour du mois suivant la période de deux ans après la date d'entrée en vigueur de l'acte d'exécution visé à l'article 22 ter du présent règlement, si les canaux de communication visés à l'article 22 bis, paragraphe 1, ne sont pas encore disponibles pour un échange direct entre elles.

11. Les autorités nationales compétentes peuvent continuer à fournir des informations autrement que de manière semi-automatique conformément à l'article 22 bis, paragraphe 3, jusqu'au premier jour du mois suivant la période de deux ans après la date d'entrée en vigueur de l'acte d'exécution visé à l'article 22 ter du présent règlement, si les exigences techniques ne sont pas encore en place.».

11) L'annexe suivante est ajoutée:

«ANNEXE III

a) Informations permettant d'identifier la personne soupçonnée, accusée, condamnée ou acquittée

Pour une personne physique:

- le nom de famille;
- le ou les prénoms;

- les pseudonymes éventuels;
- la date de naissance;
- le lieu de naissance (ville et pays);
- la ou les nationalités;
- le document d'identité (type et numéro du document);
- le sexe;
- le lieu de résidence.

Pour une personne morale:

- la dénomination commerciale;
- la forme juridique;
- le lieu du siège social.

Pour les personnes physiques et morales:

- les numéros de téléphone;
- les adresses électroniques;
- les informations sur les comptes détenus auprès de banques ou d'autres institutions financières.

b) Informations relatives à l'infraction terroriste:

- les informations concernant les personnes morales impliquées dans la préparation ou la commission d'une infraction terroriste;
- la qualification juridique de l'infraction en vertu du droit national;
- la forme d'infraction grave applicable figurant sur la liste visée à l'annexe I;
- toute affiliation à un groupe terroriste;
- le type de terrorisme, par exemple djihadisme, séparatisme, terrorisme de gauche ou terrorisme de droite;
- le résumé de l'affaire.

c) Informations relatives aux procédures nationales:

- l'état d'avancement de ces procédures;
- le Parquet compétent;
- le numéro de l'affaire;
- la date d'ouverture des poursuites judiciaires officielles;
- les liens avec d'autres affaires pertinentes.

d) Informations complémentaires permettant d'identifier le suspect:

- les données dactyloscopiques qui ont été recueillies conformément au droit national à l'occasion de procédures pénales;
- les photographies.».

Article 2

Modifications de la décision 2005/671/JAI

La décision 2005/671/JAI est modifiée comme suit:

- 1) À l'article 1^{er}, le point c) est supprimé.
- 2) L'article 2 est modifié comme suit:
 - a) le paragraphe 2 est supprimé;

b) le paragraphe 3 est remplacé par le texte suivant:

«3. Chaque État membre prend les mesures nécessaires pour veiller à ce qu'au moins les informations visées au paragraphe 4 concernant les enquêtes pénales pour infractions terroristes, qui intéressent ou sont susceptibles d'intéresser deux États membres ou plus et sont recueillies par l'autorité compétente, soient transmises à Europol, conformément au droit national et au règlement (UE) 2016/794 du Parlement européen et du Conseil (*).

(*) Règlement (UE) 2016/794 du Parlement européen et du Conseil du 11 mai 2016 relatif à l'Agence de l'Union européenne pour la coopération des services répressifs (Europol) et remplaçant et abrogeant les décisions du Conseil 2009/371/JAI, 2009/934/JAI, 2009/935/JAI, 2009/936/JAI et 2009/968/JAI (JO L 135 du 24.5.2016, p. 53).»;

c) le paragraphe 5 est supprimé.

Article 3

Entrée en vigueur

Le présent règlement entre en vigueur le vingtième jour suivant celui de sa publication au *Journal officiel de l'Union européenne*.

Le présent règlement est obligatoire dans tous ses éléments et directement applicable dans les États membres conformément aux traités.

Fait à Strasbourg, le 4 octobre 2023.

Par le Parlement européen

La présidente

R. METSOLA

Par le Conseil

Le président

J. M. ALBARES BUENO