



# GLACY-e

## Global Action on Cybercrime Enhanced Action Globale Renforcée sur la Cybercriminalité

### RÉSUMÉ DU PROJET

Version 24 novembre 2023

Titre / numéro du projet : GLACY-e (3399) - Action Globale Renforcée sur la Cybercriminalité - Projet conjoint de l'Union Européenne et du Conseil de l'Europe

Zone du projet : Plusieurs pays d'Afrique, d'Asie, du Pacifique et d'Amérique Latine

Durée de l'enquête : 30 mois (1er août 2023 - 31 janvier 2026)

Budget : 5,556,000 EUR

Financement : Projet conjoint de l'Union Européenne (Instrument de voisinage, de développement et de coopération internationale - NDICI – Global Europe) et du Conseil de l'Europe

Mise en œuvre : Bureau de programme du Conseil de l'Europe sur la Cybercriminalité (C-PROC) et INTERPOL

### CONTEXTE

Le projet GLACY-e (Action Globale Renforcée sur la Cybercriminalité), lancé en décembre 2023, est un projet conjoint de l'Union Européenne et du Conseil de l'Europe, financé par l'Union Européenne dans le cadre de l'instrument de voisinage, de développement et de coopération internationale - NDICI – Global Europe et le Conseil de l'Europe, et mis en œuvre par le Conseil de l'Europe.

L'objectif global de GLACY-e est de renforcer les capacités des États du monde entier à appliquer la législation sur la cybercriminalité et les preuves électroniques, et d'améliorer leurs capacités à coopérer efficacement au niveau international dans ce domaine et à favoriser la coopération Sud-Sud. Dans le cadre de cet objectif global, le projet met en œuvre des activités dans le monde entier à travers quatre objectifs spécifiques : (1) législation, politiques et stratégies, (2) capacités des autorités de police, (3) capacités de la justice pénale, et (4) capacités des pôles régionaux. Le deuxième objectif est mis en œuvre par INTERPOL par l'intermédiaire de son Complexe mondial pour l'innovation, à la suite d'un partenariat stratégique conclu entre le Conseil de l'Europe et INTERPOL.

Huit pays d'Afrique, d'Asie/Pacifique et d'Amérique latine : Le Chili, la République Dominicaine, le Ghana, le Sénégal, le Sri Lanka, les Philippines, l'île Maurice et les Tonga servent agissent en tant que pôles régionaux et de multiplicateurs pour partager l'expérience, les outils et les bonnes pratiques avec les pays de leur région respective.

S'appuyant sur l'expertise et l'expérience acquises par les pôles régionaux dans le cadre du projet précédent GLACY+, GLACY-e répond aux besoins spécifiques des pays sélectionnés - des États du Sud qui sont déjà parties à la Convention sur la cybercriminalité ou qui ont demandé à y adhérer et ont été invités.

D'autres pays peuvent bénéficier d'un soutien sur demande, notamment pour mettre leur législation nationale en conformité avec les normes de la Convention de Budapest sur la cybercriminalité et ses Protocoles.

### CONTACTS

Catalina STROE  
Cheffe de projet GLACY-e  
Conseil de l'Europe  
[Catalina.STROE@coe.int](mailto:Catalina.STROE@coe.int)

Alexander SEGER  
Chef de division Cybercriminalité  
Conseil de l'Europe  
[Alexander.SEGER@coe.int](mailto:Alexander.SEGER@coe.int)

[www.coe.int/cybercrime](http://www.coe.int/cybercrime)

## OBJECTIFS ET RESULTATS ATTENDUS

<b>Objectif du projet</b>	<b>Renforcer les capacités des États du monde entier à appliquer la législation sur la cybercriminalité et les preuves électroniques, et améliorer leurs capacités à coopérer efficacement au niveau international dans ce domaine et à favoriser la coopération sud-sud.</b>
<b>Objectif 1</b>	<b>Promouvoir l'adoption et la mise en œuvre d'une législation, des politiques et des stratégies cohérentes en matière de cybercriminalité</b>
Résultat 1.1	Renforcement de la législation et des stratégies en matière de cybercriminalité, des preuves électroniques et des dispositions relatives à la protection des données, conformément à la Convention de Budapest et à ses Protocoles, ainsi qu'aux normes relatives à l'État de droit et aux droits de l'homme, dans les pays pivots, les pays sélectionnés et d'autres pays.
Résultat 1.2	Le dialogue entre les parties prenantes nationales sur l'élaboration et la mise en œuvre d'une législation, des politiques et des stratégies en matière de cybercriminalité et des preuves électroniques dans les pôles régionaux, les pays sélectionnés et d'autres pays est renforcé.
Résultat 1.3	Renforcement du dialogue politique et stratégique et de la coopération en matière de cybercriminalité entre les organisations internationales et régionales
<b>Objectif 2</b>	<b>Renforcer la capacité des autorités de police à enquêter sur la cybercriminalité et à s'engager dans une coopération efficace entre les services de police.</b>
Résultat 2.1	Les unités chargées de la cybercriminalité et de la criminalistique informatique au sein des autorités policières sont renforcées dans les pôles régionaux et les pays sélectionnés, et la coopération policière internationale est plus efficace.
Résultat 2.2	Les autorités de police dans les pôles régionaux et les pays sélectionnés sont formées en matière d'enquêtes de base sur la cybercriminalité et à la criminalistique informatique, et des stratégies de formation sont disponibles dans les pôles régionaux et les pays sélectionnés.
Résultat 2.3	Renforcement de la coopération interinstitutionnelle dans les pôles régionaux et les pays sélectionnés entre les autorités de police et les unités d'enquête financière (FIU) et les procureurs sur les produits du crime en ligne afin d'assurer une confiscation, une localisation et un recouvrement efficaces des avoirs.
<b>Objectif 3</b>	<b>Permettre aux autorités de justice pénale d'appliquer la législation, de poursuivre et de juger les dossiers de cybercriminalité et des preuves électroniques et de s'engager dans la coopération internationale, conformément aux normes internationales en matière de droits de l'homme et d'État de droit.</b>
Résultat 3.1	Les autorités de justice pénale disposent des connaissances et des compétences nécessaires en matière de cybercriminalité et de preuves électroniques dans les pôles régionaux et les pays sélectionnés.
Résultat 3.2	La coopération judiciaire internationale et le renforcement des capacités entre pairs en matière de cybercriminalité et des preuves électroniques sont améliorés dans les pôles régionaux et les pays sélectionnés, notamment par le renforcement de la communauté internationale/du réseau de formateurs judiciaires nationaux.
Résultat 3.3	Amélioration de la réponse de la justice pénale aux défis liés à la pandémie de COVID-19 et à ses conséquences, ainsi qu'aux questions émergentes liées à la cybercriminalité et aux preuves électroniques.
<b>Objectif 4</b>	<b>Renforcer les capacités des pôles régionaux en matière de cybercriminalité et des preuves électroniques dans leur région et promouvoir leur rôle régional dans la coopération sud-sud.</b>
Résultat 4.1	Les centres de formation policière et judiciaire et d'autres entités des pôles régionaux proposent des programmes de renforcement des capacités en matière de cybercriminalité et des preuves électroniques au niveau régional.
Résultat 4.2	Renforcement des capacités des autorités de police et de justice pénale des pôles régionaux à servir comme des centres d'expertise et d'expérience, et à partager les meilleures pratiques en matière d'enquête, de poursuite et de jugement sur les dossiers de cybercriminalité et les dossiers impliquant des preuves électroniques aux niveaux régional et international.