GLACY+
Global Action on Cybercrime Extended
Action Globale sur la Cybercriminalité Elargie

Version 14 février 2020

Résumé du projet

Titre du projet :	GLACY + (3148) – Action Globale sur la Cybercriminalité Élargie – projet conjoint de l'Union européenne et du Conseil de l'Europe
Zones géographiques :	Plusieurs pays d'Afrique, de la région Asie-Pacifique et d'Amérique latine
Durée :	96 mois (1 mars 2016 – 28 février 2024)
Budget:	18,890,000 EUR
Financement :	Projet conjoint de l'Union européenne (Instrument contribuant à la paix et à la stabilité, IcPS) et du Conseil de l'Europe
Implémentation :	Bureau de programme du Conseil de l'Europe sur la cybercriminalité (C-PROC) et INTERPOL

CONTEXTE

Le projet GLACY + (Action Globale sur la Cybercriminalité Élargie), lancé en octobre 2016, est un projet conjoint de l'Union européenne et du Conseil de l'Europe financé dans le cadre de l'Instrument contribuant à la paix et à la stabilité (IcPS) et a pour objectif global de renforcer les capacités des États du monde entier à appliquer la législation sur la cybercriminalité et les preuves électroniques et à renforcer leurs capacités de coopération internationale efficace dans ce domaine.

Le projet compte actuellement 12 pays prioritaires (Cabo Verde, Chili, Costa Rica, République dominicaine, Ghana, Ile Maurice, Maroc, Nigéria, Philippines, Sénégal, Sri Lanka et Tonga), dont certains peuvent être utilisés comme centres régionaux pour diffuser et multiplier les effets du projet. L'objectif à cet égard est d'augmenter le nombre de pays prioritaires ou centres régionaux à 15 pays.

Bien que le projet cible principalement les pays susmentionnés, il est également ouvert à la mise en œuvre d'activités dans d'autres pays, sur demande, en particulier en ce qui concerne la conformité législative entre la législation nationale et la Convention de Budapest.

Le projet GLACY + met en œuvre des activités dans le monde entier à travers trois objectifs spécifiques, à savoir (1) les politiques et stratégies, (2) les capacités des forces de l'ordre et (3) les capacités de la justice pénale.

Le deuxième objectif du projet est mis en œuvre par le Complexe mondial pour l'innovation d'INTERPOL (IGCI), dans le cadre d'un accord avec le Conseil de l'Europe.

OBJECTIF ET RESULTATS ATTENDUS

But du projet	**Renforcer les capacités des Etats du monde entier à application la législation sur la cybercriminalité et la preuve électronique et renforcer leurs capacités pour une coopération internationale effective dans ce domaine.**
Objectif 1	**Promouvoir des politiques et stratégies cohérentes en matière de cybercriminalité et de cybersécurité.**
Résultat 1.1	Les politiques et stratégies en matière de cybercriminalité et de cybersécurité sont renforcées dans au moins 20 pays, y compris les aspects pertinents de la cybersécurité et les partenariats avec le secteur privé, et l'expérience est partagée avec d'autres pays.
Résultat 1.2	Renforcement du dialogue politique et de la coopération sur la cybercriminalité entre les pays prioritaires et leurs régions, les organisations internationales et régionales, et maximisation des synergies avec les projets financés par l'UE (notamment financés par l'IcSP) développés dans les zones de projet.
Résultat 1.3	La législation sur les preuves électroniques en matière de cybercriminalité et les dispositions connexes en matière de protection des données sont renforcées conformément à la Convention de Budapest et à ses protocoles ainsi qu'à l'état de droit et aux normes relatives aux droits de l'homme dans les pays prioritaires et des réformes sont engagées dans d'autres pays.
Objectif 2	**Renforcer la capacité des autorités de police en matière d'enquête sur la cybercriminalité et pour entamer une coopération efficace de police à police, entre services de police ainsi qu'avec des services chargés de lutter contre la cybercriminalité, en Europe et dans d'autres régions.**
Résultat 2.1	Evaluations/passages en revue cyber (initiaux et finaux) des capacités dont disposent les forces de l'ordre dans les pays prioritaires.
Résultat 2.2	Les services d'investigations numériques sont renforcés dans des pays prioritaires et l'expérience est partagée avec d'autres pays.
Résultat 2.3	Les pays prioritaires sont dotés de stratégies de formation pour les forces de l'ordre, y compris l'accès à des matériels de formation de l'ECTEG.
Résultat 2.4	Au moins 1,000 agents des forces de l'ordre sont formés aux investigations minimales en matière de cybercriminalité et aux bases de l'analyse informatique légale ainsi qu'aux conditions à remplir dans ce domaine en matière d'Etat de droit.
Résultat 2.5	La coopération internationale entre services de police sur la cybercriminalité et la preuve électronique est plus efficace.
Résultat 2.6	Renforcement de la coopération interinstitutionnelle des unités de lutte contre la cybercriminalité, des enquêteurs financiers et des unités de renseignement financier pour la recherche, la saisie et la confiscation des produits du crime en ligne
Objectif 3	**Permettre aux autorités de justice pénale d'appliquer la législation et de poursuivre et juger des affaires de cybercriminalité avec des preuves électroniques, ainsi que de s'engager dans la coopération internationale.**
Résultat 3.1	Evaluations des capacités de la justice pénale pour des pays prioritaires.
Résultat 3.2	Les académies de formation judiciaire des pays prioritaires dispensent une formation sur la cybercriminalité et les preuves électroniques dans le cadre de leurs programmes réguliers et l'expérience est partagée avec d'autres pays.
Résultat 3.3	Renforcement des institutions et amélioration des procédures de coopération judiciaire internationale en matière de cybercriminalité et de preuve électronique dans au moins 20 pays et partage d'expérience avec d'autres pays.
Résultat 3.4	Des centres de formation, des établissements universitaires et autres entités offrant des programmes de renforcement des capacités en matière de justice pénale de portée régionale sont renforcés et la formation sur la cybercriminalité et les preuves électroniques est rationalisée dans les programmes respectifs.