

អង្គការទិន្នន័យអំពីការអភិវឌ្ឍ

សន្តិសុខសាយប័រនៅកម្ពុជា៖ ដំណើរការអភិវឌ្ឍនាពេលបច្ចុប្បន្ន និងបញ្ហាប្រឈមនាពេលខាងមុខ

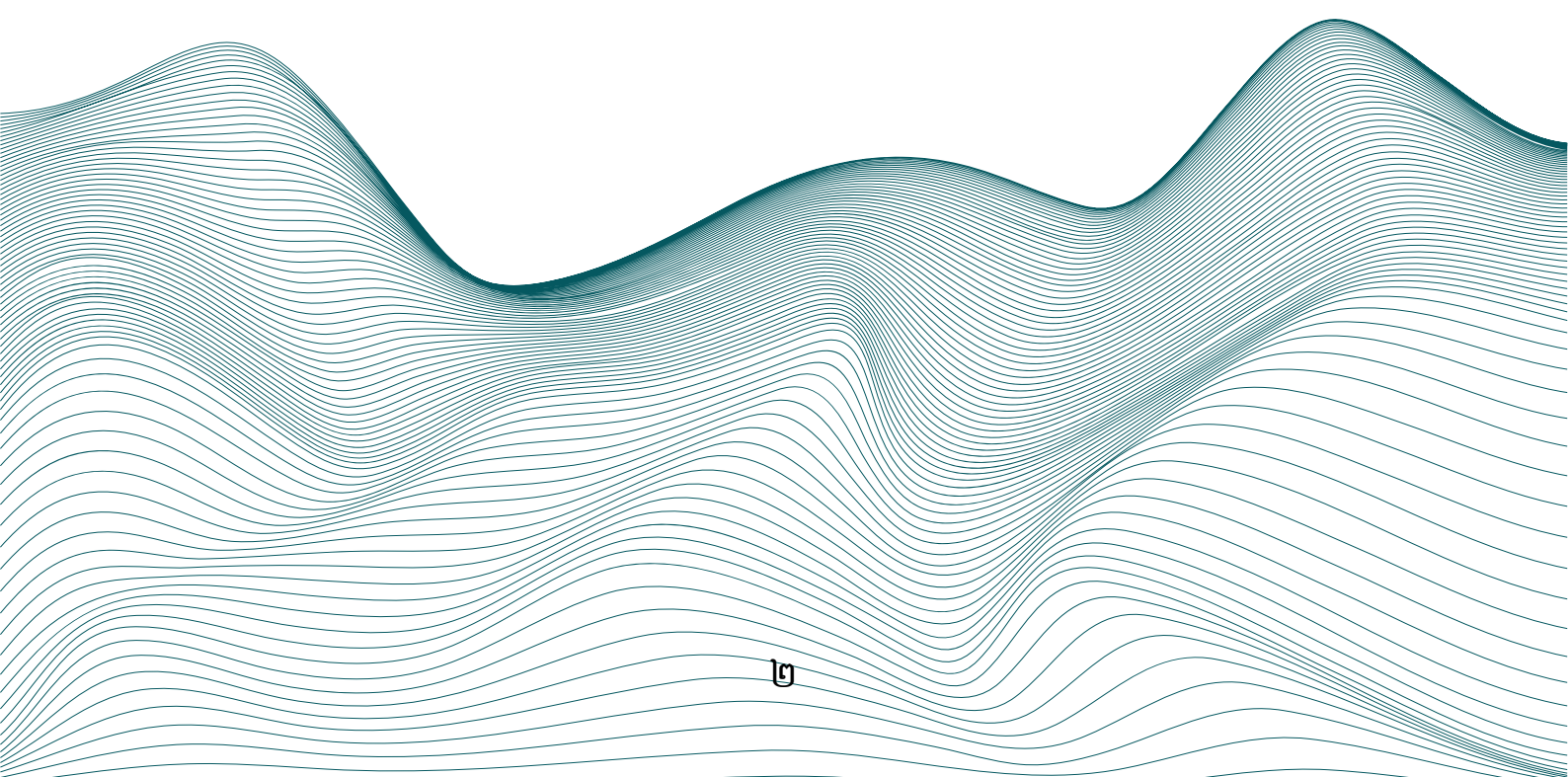
ខែមីនា ឆ្នាំ២០២៣



អង្គការទិន្នន័យអំពីការអភិវឌ្ឍ
Open Development Cambodia Organization

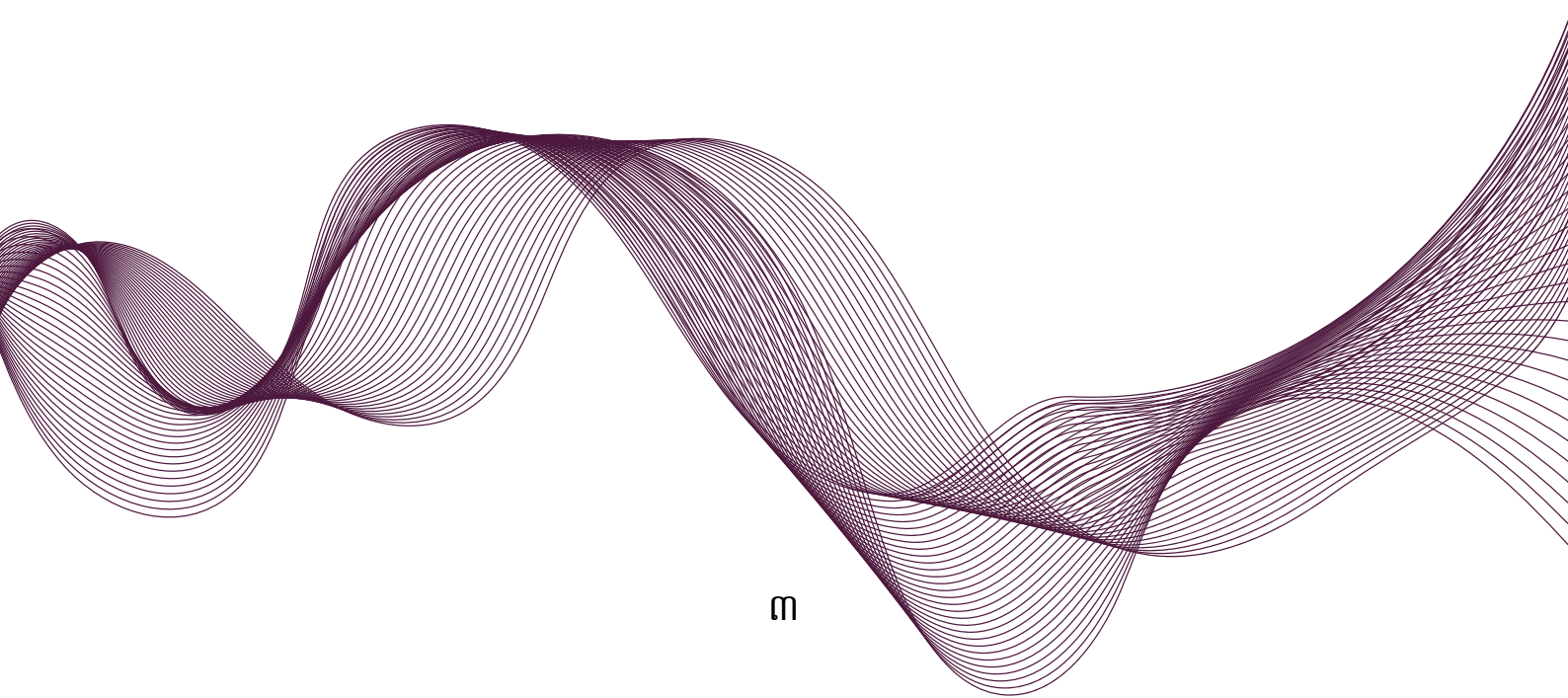
សេចក្តីសង្ខេប

ដំណើរការនៃឌីជីថលភាវូបនីយកម្មនៅប្រទេសកម្ពុជាបានចាប់ផ្តើមរយៈពេលពីរទសវត្សរ៍មកហើយ ហើយវាបានផ្លាស់ប្តូរខ្លួនយ៉ាងឆាប់រហ័សក្នុងវិស័យសង្គម នយោបាយ និងសេដ្ឋកិច្ចជាមួយនឹង ឱកាសថ្មីៗមួយចំនួនក្នុងការអភិវឌ្ឍប្រទេស។ ទោះយ៉ាងណាក៏ដោយ ភាពពេញនិយម របស់អ៊ីនធឺណិត ឧបករណ៍ឌីជីថល និងប្រព័ន្ធផ្សព្វផ្សាយឌីជីថលផ្សេងៗក៏នាំមកនូវបញ្ហាប្រឈម ថ្មីៗផងដែរ ពោលគឺបញ្ហាសន្តិសុខនៅក្នុងវិស័យឌីជីថល។ ដើម្បីដោះស្រាយបញ្ហាដែលកើតមាន ក្នុងយុគសម័យឌីជីថល រាជរដ្ឋាភិបាលកម្ពុជាបានដាក់ចេញនូវវិធានការផ្លូវច្បាប់ថ្មី ដើម្បីដោះស្រាយឧក្រិដ្ឋកម្មតាមអ៊ីនធឺណិត និងធ្វើឱ្យលំហឌីជីថលកាន់តែមានសុវត្ថិភាពជាងមុន។ យ៉ាងណាក៏ដោយ វានៅតែមានកន្លែងក្នុងការកែលម្អ។ អត្ថបទនេះធ្វើការពិនិត្យទៅលើច្បាប់សំខាន់ៗ និងវិធានការផ្លូវច្បាប់ដែលត្រូវបានអនុម័តដោយរដ្ឋាភិបាលកម្ពុជា ដើម្បីវាយតម្លៃវឌ្ឍនភាពនៃសន្តិសុខសាយបំរែដែលបានកើតឡើងនៅក្នុងប្រទេស។ អត្ថបទនេះបង្ហាញថាយើងនៅតែមានចន្លោះប្រហោងកន្លែងសម្រាប់កែលម្អ ខណៈពេលដែល ដំណើរការល្អប្រសើរមួយភាគធំត្រូវបានធ្វើឡើង នៅក្នុងទសវត្សរ៍ចុងក្រោយនេះក៏ដោយ។ រដ្ឋាភិបាលកម្ពុជាគួរតែធ្វើការយ៉ាងជិតស្និទ្ធជាមួយអ្នកពាក់ព័ន្ធផ្សេងៗក្នុងសង្គមស៊ីវិល ដើម្បីធ្វើឱ្យសេចក្តីព្រាងច្បាប់សន្តិសុខសាយបំរែនេះជាដំណើរការបង្កើតរួមគ្នាដែលគិតគូរពីទស្សនៈ និងតម្រូវការរបស់ភាគីផ្សេងៗឱ្យបានច្រើនតាមដែលអាចធ្វើទៅបាន នោះទើបច្បាប់សន្តិសុខសាយបំរែនឹងមាននិរន្តរភាព។



មាតិកា

- ១. បរិបទ.....៤
 - ១.១. ឌីជីថលភារូបនីយកម្មនៅប្រទេសកម្ពុជា.....៤
 - ១.២. សន្តិសុខសាយបំរះ បញ្ហាប្រឈមសំខាន់នៅក្នុងយុគសម័យឌីជីថល.....៦
 - ១.៣. ភាពបន្ទាន់សម្រាប់តម្រូវការបន្ថែមនៃច្បាប់សន្តិសុខសាយបំរះ.....៨
- ២. ច្បាប់សន្តិសុខសាយបំរះ.....៩
 - ២.១. ច្បាប់ស្តីពីការគ្រប់គ្រងវិស័យទូរគមនាគមន៍ជាតិ.....១០
 - ២.២. ច្បាប់ស្តីពីឧក្រិដ្ឋកម្មតាមអ៊ីនធឺណិត.....១១
 - ២.៣. អនុក្រឹត្យស្តីពីការបង្កើតអាជ្ញាធរជាតិប្រយុទ្ធប្រឆាំងនឹងឧក្រិដ្ឋកម្មតាមអ៊ីនធឺណិត....១៣
 - ២.៤. ប្រកាសស្តីពីការគ្រប់គ្រងសន្តិសុខសាយបំរះ.....១៤
 - ២.៥. អនុក្រឹត្យស្តីពីការបង្កើតគណៈកម្មាធិការជាតិសន្តិសុខសាយបំរះ.....១៥
- ៣. កិច្ចពិភាក្សា៖ ជំហានបន្ទាប់?.....១៧
- ៤. សេចក្តីសន្និដ្ឋាន.....១៨
- គន្ថនិទ្ទេស.....២០



១. បរិបទ

ប្រទេសកម្ពុជាក៏ជាប្រទេសមួយដែលមាននិន្នាការភារុបនីយកម្មឌីជីថលសកល ដោយធ្វើឱ្យអ៊ីនធឺណិតក្លាយជាធាតុស្នូល នៃប្រព័ន្ធសង្គម សេដ្ឋកិច្ច និងនយោបាយរបស់ខ្លួន។ ប្រទេសនេះបានមើលឃើញពីរបៀបដែលអ៊ីនធឺណិត និងទូរស័ព្ទដៃឆ្លាតវៃបានក្លាយជាការពេញនិយមយ៉ាងខ្លាំង នៅក្នុងប្រទេសចាប់តាំងពីចុងទសវត្សរ៍ឆ្នាំ២០០០ និងជាពិសេសចាប់តាំងពីដើមទសវត្សរ៍ឆ្នាំ២០១០ មក។ ការអភិវឌ្ឍយ៉ាងឆាប់រហ័សនៃវិស័យឌីជីថលបាននាំមកជាមួយនឹងលទ្ធផលវិជ្ជមានមួយភាគធំ ដូចជាការចូលប្រើប្រាស់ជាអចិន្ត្រៃយ៍របស់មនុស្សទៅកាន់ប្រភពព័ត៌មានផ្សេងៗពីបណ្តាញក្នុងប្រទេស និងអន្តរជាតិ។ នៅក្នុងបរិបទនេះ បញ្ហាប្រឈមដូចជាឧក្រិដ្ឋកម្មតាមអ៊ីនធឺណិតបានកើតឡើង ហើយវាក៏ជាប្រភេទបញ្ហាលើបញ្ហា។ ម៉្យាងវិញទៀត ឧក្រិដ្ឋកម្មតាមអ៊ីនធឺណិតគឺជាបញ្ហាប្រឈមមួយ ដោយសារតែវាសំដៅទៅលើសំណុំនៃសកម្មភាពដែលកើតឡើង នៅក្នុងវិស័យឌីជីថលដែលមានលក្ខណៈខុសច្បាប់ ប៉ុន្តែប្រព័ន្ធច្បាប់មិនទាន់បានត្រៀមខ្លួនរួចជាស្រេចដើម្បីទប់ទល់ នឹងការអភិវឌ្ឍយ៉ាងឆាប់រហ័សនៃវិស័យឌីជីថល ដែលរួមមានឧបករណ៍ឌីជីថល និងប្រព័ន្ធផ្សព្វផ្សាយថ្មីៗនោះទេ។ ជាការឆ្លើយតប រដ្ឋាភិបាលកម្ពុជាបានបង្កើតឬព្រាងច្បាប់ថ្មី ដើម្បីដោះស្រាយបញ្ហាប្រឈមឌីជីថលថ្មីៗនៃយុគសម័យអ៊ីនធឺណិត ដែលជាការរួមចំណែកដល់ការអភិវឌ្ឍបណ្តាញអ៊ីនធឺណិត ជាមួយនឹងច្បាប់ដើម្បីដោះស្រាយឧក្រិដ្ឋកម្មតាមអ៊ីនធឺណិត។ អត្ថបទនេះសិក្សាពីវឌ្ឍនភាពនេះ ដោយមើលលើទិដ្ឋភាពទូទៅនៃបទប្បញ្ញត្តិចំនួនប្រាំ ហើយក៏ចង្អុលបង្ហាញថា ទោះបីជាវឌ្ឍនភាពសំខាន់ៗត្រូវបានរួមបញ្ចូលក្នុងការធ្វើការសម្រេចដើម្បីដោះស្រាយឧក្រិដ្ឋកម្មតាមអ៊ីនធឺណិតក៏ដោយ ក៏ច្បាប់ឌីជីថលថ្មីនេះត្រូវតែមានភាពជាក់លាក់បន្ថែមទៀត ដោយពិចារណាលើតម្រូវការរបស់ស្ថាប័នជាច្រើន ហើយត្រូវតែពង្រឹង និងពិចារណាលើទស្សនៈរបស់អ្នកពាក់ព័ន្ធទាំងអស់ដើម្បីបង្កើននិរន្តរភាពរបស់ខ្លួន។

១.១. ឌីជីថលភារុបនីយកម្មនៅប្រទេសកម្ពុជា

ប្រទេសកម្ពុជាបានឆ្លងកាត់ការផ្លាស់ប្តូរវិស័យឌីជីថលយ៉ាងឆាប់រហ័ស។ កត្តាសំខាន់មួយដែលជំរុញដល់ឌីជីថលភារុបនីយកម្មរបស់ប្រទេសកម្ពុជា គឺការបង្កើនលទ្ធភាពនៃការប្រើប្រាស់អ៊ីនធឺណិត។ យោងទៅតាម Kemp (ឆ្នាំ២០២៣) ការជ្រៀតចូលនៃអ៊ីនធឺណិតនៅក្នុងប្រទេសកម្ពុជាមានអ្នកប្រើប្រាស់ចំនួន ៦៧,៥% (១១,៣៧លាននាក់) នៅដើមឆ្នាំ២០២៣។ ចន្លោះឆ្នាំ២០២២ និង ២០២៣ អ្នកប្រើប្រាស់អ៊ីនធឺណិតក្នុងប្រទេស បានកើនឡើង ៦,៧% ឬ ៧១៤.០០០។ នៅដើមឆ្នាំ២០២៣ ដូចគ្នា កម្ពុជាមានអ្នកប្រើប្រាស់អ៊ីនធឺណិតតាមទូរស័ព្ទចល័តសរុបចំនួន ២២,១៦លាននាក់ ដែលចំនួននេះគឺស្មើនឹង ១៣១,៥% នៃចំនួនប្រជាជនសរុបនៅក្នុងប្រទេស។

បើនិយាយឱ្យកាន់តែច្បាស់ ការពេញនិយមនៃបណ្តាញទំនាក់ទំនងសង្គម (SNS) បានកើនឡើងយ៉ាងឆាប់រហ័ស។ គិតត្រឹមខែមករា ឆ្នាំ២០២៣ ប្រទេសកម្ពុជាមានអ្នកប្រើប្រាស់ប្រព័ន្ធផ្សព្វផ្សាយសង្គមចំនួន ១០,៩៥លាននាក់ ឬស្មើនឹង ៦៥,០% នៃចំនួនប្រជាជនសរុប។ ហ្វេសប៊ុកបាន

បង្ហាញខ្លួន និងរួមជាវេទិកាប្រព័ន្ធផ្សព្វផ្សាយសង្គមដ៏ពេញនិយមបំផុត នៅក្នុងប្រទេស។ យោងតាមក្រុមហ៊ុន Meta បណ្តាញហ្វេសប៊ុកមានអ្នកប្រើប្រាស់ចំនួន ១០,៤៥លាននាក់នៅក្នុងប្រទេសនៅដើមឆ្នាំ២០២៣។ ក្រៅពីភាពលេចធ្លោរបស់វានៅក្នុងទិដ្ឋភាពនៃវេទិកាប្រព័ន្ធផ្សព្វផ្សាយ សង្គមនៅក្នុងប្រទេស ទិន្នន័យក៏បានបង្ហាញផងដែរថា សក្តានុពលនៃការផ្សាយពាណិជ្ជកម្មរបស់ ហ្វេសប៊ុក នៅកម្ពុជាបានថយចុះជិត ១០% ចន្លោះឆ្នាំ២០២២ និង ២០២៣។ ការថយចុះចំនួនអ្នកប្រើប្រាស់ហ្វេសប៊ុក ត្រូវបានពន្យល់ដោយផ្នែកលើផ្នែកខ្លះៗថា ដោយសារតែមានវត្តមាននៃបណ្តាញទំនាក់ទំនងសង្គមផ្សេងទៀត និងមុខងារថ្មីដែលពួកគេផ្តល់ជូន។ នៅដើមឆ្នាំ២០២៣ Instagram មានអ្នកប្រើប្រាស់ចំនួន ១,៧៥លាននាក់ ក្នុងប្រទេសកម្ពុជា ហើយក៏ដូចជាហ្វេសប៊ុកដែរ អ្នកប្រើប្រាស់បានថយចុះ ១៤,៦% ឬ ៣០០,០០០ ចន្លោះឆ្នាំ២០២២ និង ២០២៣។ TikTok មានអ្នកប្រើប្រាស់ជាង ៧លាននាក់ ដែលមានអាយុចាប់ពី ១៨ឆ្នាំឡើងទៅនៅដើមឆ្នាំ២០២៣។

បរិបទនៃការអភិវឌ្ឍវិស័យឌីជីថលគឺជារឿងចាំបាច់ ព្រោះវាបានពន្យល់ពីផលប៉ះពាល់ជាច្រើននៅក្នុងសង្គម នយោបាយ និងសេដ្ឋកិច្ចក្នុងប្រទេស។ ការកើនឡើងនៃអ៊ីនធឺណិត និងបណ្តាញទំនាក់ទំនងសង្គមជាច្រើនបានជះឥទ្ធិពលយ៉ាង ខ្លាំងដល់សង្គមកម្ពុជា។ នៅក្នុងសង្គម វិស័យឌីជីថលបានអនុញ្ញាតឱ្យប្រជាពលរដ្ឋមិនត្រឹមតែបង្ហាញចែករំលែកអំពីជីវិត ប្រចាំថ្ងៃរបស់ពួកគេប៉ុណ្ណោះទេ ប៉ុន្តែក៏ដើម្បីទទួលបានព័ត៌មានទូលំទូលាយពីប្រទេសកម្ពុជា និងពីក្រៅប្រទេស រួមទាំងប្លុកដែលសរសេរដោយសកម្មជនដែលបង្ហាញអំពីបញ្ហាមួយចំនួនដែលប៉ះពាល់ដល់ប្រទេស និងទីក្រុងរបស់ពួកគេផងដែរ (Phong et al., 2016)។ ប្រព័ន្ធអ៊ីនធឺណិតក៏បានធ្វើបដិវត្តនាករនយោបាយរបស់ប្រទេសកម្ពុជាជាមួយប្រជាពលរដ្ឋដែលពង្រីកការយល់ដឹងអំពីការអភិវឌ្ឍនយោបាយចុងក្រោយបង្អស់ តួនាទីរបស់គណបក្សប្រឆាំង និងទិដ្ឋភាពទូទៅ ដែលធ្វើឱ្យរដ្ឋាភិបាលកាន់តែមានទំនួលខុសត្រូវតាមរយៈ ការទាមទារឱ្យមានអភិបាលកិច្ចកាន់តែប្រសើរឡើងទាក់ទងនឹងសេវាសាធារណៈ និងអាចតាមដានអំពីវឌ្ឍនភាព (វង្ស និង ហុក 2018)។ តាមទស្សនៈពុទ្ធសាស្ត្រ វិស័យឌីជីថលបានបើកទ្វារដល់ឱកាសជាច្រើនសម្រាប់អាជីវកម្មរួម និងសហគ្រិនដែលទទួលយកអ៊ីនធឺណិតជាយន្តការសំខាន់មួយក្នុងការលើកកម្ពស់អាជីវកម្មរបស់ពួកគេ និងឈានដល់អ្នកប្រើប្រាស់ថ្មីៗដែលមានសក្តានុពលទៅលើផលិតផលរបស់ពួកគេ (អូឌីស៊ី, n.d)។

ដោយមើលឃើញពីសមត្ថភាពរបស់អ៊ីនធឺណិតក្នុងការរៀបចំវិស័យសាធារណៈ និងឯកជន រាជរដ្ឋាភិបាលកម្ពុជា បានបញ្ជាក់អំពីការអនុវត្តគោលនយោបាយថ្មី ដើម្បីបង្កើនលទ្ធភាពប្រើប្រាស់អ៊ីនធឺណិត និងលើកកម្ពស់ការអភិវឌ្ឍនៃរដ្ឋាភិបាលឌីជីថល និងវិស័យសេដ្ឋកិច្ច។ រាជរដ្ឋាភិបាលបានចាត់ទុកឌីជីថលភារៈសំខាន់សម្រាប់ប្រទេសចាប់តាំងពីការចាប់ផ្តើមមក។ ក្រោមការបកស្រាយរបស់ក្រសួងទូរគមនាគមន៍ និងប្រៃសណីយ៍ “ក្របខ័ណ្ឌគោលនយោបាយសេដ្ឋកិច្ច និងសង្គមឌីជីថលកម្ពុជា ឆ្នាំ២០២១-២០៣៥ (MPTC, 2022) ត្រូវបានបង្កើតឡើងដោយសសរស្តម្ភសំខាន់ៗចំនួនបី៖ ពលរដ្ឋឌីជីថល រដ្ឋាភិបាលឌីជីថល និងពុទ្ធសាស្ត្រឌីជីថល ដែលក្នុងនោះការកសាងរដ្ឋាភិបាលឌីជីថលត្រូវចាប់ផ្តើមដំបូងគេ ដើម្បីលើកកម្ពស់ការអនុវត្ត និងការប្រើប្រាស់បច្ចេកវិទ្យាឌីជីថល និងការផ្លាស់ប្តូរឌីជីថលនៅក្នុងសេដ្ឋកិច្ច និងសង្គមទាំងមូល”។ ការបង្កើតយុទ្ធសាស្ត្រឌីជីថលបានអនុញ្ញាត

ឱ្យមានការកែលម្អប្រទេសក្នុងវិស័យជាច្រើន ដោយប្រើប្រាស់ឧបករណ៍ឌីជីថល និងប្រព័ន្ធផ្សព្វផ្សាយជាជំនួយ រួមទាំងការអប់រំដែលប្រសើរឡើង កំណើនសេដ្ឋកិច្ច និងការពង្រឹងទំនាក់ទំនង។ កំណើននេះត្រូវបានសម្របសម្រួលដោយគោលនយោបាយរបស់រដ្ឋាភិបាលដែលមានគោលបំណងកែលម្អហេដ្ឋារចនាសម្ព័ន្ធអ៊ីនធឺណិត និងកាត់បន្ថយការចំណាយលើគម្រោងទិន្នន័យ (Property Report, 2021)។ រដ្ឋាភិបាលក៏បានដាក់ចេញនូវគំនិតផ្តួចផ្តើមក្នុងការផ្តល់ការបណ្តុះបណ្តាលជំនាញឌីជីថលដល់និស្សិត និងសហគ្រិន ដោយជំរុញឱ្យមានការទទួលយកបច្ចេកវិទ្យាឌីជីថលនៅក្នុងប្រទេសផងដែរ (CADT, 2022)។

ឌីជីថលភារៈបនីយកម្មនៅប្រទេសកម្ពុជាបានជះឥទ្ធិពលជាវិជ្ជមានដល់ប្រព័ន្ធអប់រំរបស់ប្រទេស (UNESCO, 2020)។ សាលារៀន និងសាកលវិទ្យាល័យជាច្រើនបានប្រើប្រាស់កម្មវិធីសិក្សាតាមអ៊ីនធឺណិត ដែលអនុញ្ញាតឱ្យសិស្សនិស្សិតចូលប្រើប្រាស់ធនធានអប់រំគ្រប់ទិសទីតាមរយៈការភ្ជាប់អ៊ីនធឺណិត។ វាមានសារៈសំខាន់យ៉ាងពិសេសក្នុងអំឡុងពេលជំងឺរាតត្បាតកូវីដ-១៩ ដែលបានបង្ខំឱ្យសិស្សជាច្រើនត្រូវរៀនពីផ្ទះ។ ឌីជីថលភារៈបនីយកម្មក៏បានបើកឱកាសថ្មីសម្រាប់ការរៀនពីចម្ងាយ ដែលអាចឱ្យសិស្សានុសិស្សទទួលបានការអប់រំប្រកបដោយគុណភាពពិចម្ងាយ។ ក្រៅពីការធ្វើឱ្យប្រសើរឡើងលើវិស័យអប់រំ ឌីជីថលភារៈបនីយកម្មនៅប្រទេសកម្ពុជាក៏បានជំរុញកំណើនសេដ្ឋកិច្ចផងដែរ។ ការអភិវឌ្ឍនៃសេដ្ឋកិច្ចឌីជីថលបានបង្កើតឱកាសការងារថ្មី និងអាចឱ្យអាជីវកម្មខ្នាតតូចអាចទៅដល់អតិថិជនថ្មីតាមរយៈវេទិកាពាណិជ្ជកម្មអេឡិចត្រូនិក។ រដ្ឋាភិបាលបានចាប់ផ្តើមគំនិតផ្តួចផ្តើមជាច្រើន ដើម្បីគាំទ្រដល់កំណើននៃសេដ្ឋកិច្ចឌីជីថល រួមទាំងការបង្កើតឧបករណ៍បង្កើនល្បឿននៃធុរកិច្ចថ្មី និងការបង្កើតការលើកទឹកចិត្តពន្ធសម្រាប់ក្រុមហ៊ុនបច្ចេកវិទ្យា។

សរុបមកអ៊ីនធឺណិតបានក្លាយជា ឧបករណ៍មិនអាចខ្វះបានសម្រាប់សង្គមកម្ពុជា ដែលរួមចំណែកដល់ការអភិវឌ្ឍប្រទេសលើវិស័យជាច្រើន។ យ៉ាងណាក៏ដោយ វាត្រូវតែកត់សម្គាល់ថា ការអភិវឌ្ឍនៃវិស័យឌីជីថលក៏មានបញ្ហាប្រឈមមួយចំនួនផងដែរ។ បញ្ហាទាក់ទងនឹងសន្តិសុខសាយប័រ គឺជាឧទាហរណ៍ដ៏ច្បាស់បំផុតមួយដែលត្រូវបានបកស្រាយនៅក្នុងផ្នែកបន្ទាប់។

១.២. សន្តិសុខសាយប័រ៖ បញ្ហាប្រឈមសំខាន់នៅក្នុងយុគសម័យឌីជីថល

សន្តិសុខសាយប័រ គឺជាកង្វល់ដែលកំពុងកើនឡើងនៅទូទាំងពិភពលោក ហើយប្រទេសកម្ពុជាក៏មិនមានករណីលើកលែងផងដែរ។ នៅពេលដែលកម្ពុជាមានឌីជីថលកាន់តែច្រើន ហានិភ័យនៃការវាយប្រហារតាមអ៊ីនធឺណិតក៏មានការកើនឡើង ហើយការការពារព័ត៌មានលើប្រព័ន្ធចូលប្រើដោយគ្មានការអនុញ្ញាតគឺជារឿងសំខាន់។ សន្តិសុខសាយប័រ គឺជាបញ្ហាប្រឈមដ៏សំខាន់មួយសម្រាប់ប្រទេសកម្ពុជា ហើយមានហេតុផលជាច្រើនដែលនាំឱ្យមានបញ្ហានេះ។

បញ្ហាប្រឈមចម្បងមួយនៃសន្តិសុខសាយប័រនៅកម្ពុជា គឺកង្វះការយល់ដឹងក្នុងចំណោមប្រជាជនទូទៅ (Corrado and Sakal, 2021)។ មនុស្សជាច្រើននៅក្នុងប្រទេសកម្ពុជាមាន

ចំណេះដឹងតិចតួចអំពីហានិភ័យនៃការប្រើប្រាស់អ៊ីនធឺណិត ហើយមិនសុំនឹងការអនុវត្តល្អបំផុត សម្រាប់សុវត្ថិភាពអនឡាញ។ កង្វះការយល់ដឹងនេះធ្វើឱ្យពួកគេកាន់តែងាយរងគ្រោះ ទៅនឹងការ គំរាមកំហែងតាមអ៊ីនធឺណិតដូចជា ការវាយប្រហារដោយការបោកបញ្ឆោត (phishing) ដោយ មេរោគ និងតាមរយៈការវាយប្រហារតាមអ៊ីនធឺណិតបែបវិស្វកម្មសង្គម (Social Engineering)។

បញ្ហាប្រឈមមួយទៀត គឺកង្វះអ្នកជំនាញបច្ចេកទេសក្នុងសន្តិសុខសាយប័រ (Flynn, 2019)។ កង្វះអ្នកជំនាញផ្នែកសន្តិសុខសាយប័រនៅក្នុងប្រទេសកម្ពុជា អាចបង្កការលំបាកដល់អង្គការ នានាក្នុងការអនុវត្តវិធានការសន្តិសុខដ៏រឹងមាំ។ កង្វះអ្នកជំនាញផ្នែកសន្តិសុខសាយប័រនេះ ក៏បូក ផ្សំដោយកង្វះការវិនិយោគលើការបណ្តុះបណ្តាល និងការអប់រំក្នុងវិស័យនេះផងដែរ។

លើសពីនេះទៀត ក្រៅពីកិច្ចខិតខំប្រឹងប្រែងរបស់រាជរដ្ឋាភិបាលកម្ពុជា ក្របខ័ណ្ឌច្បាប់កម្ពុជា សម្រាប់សន្តិសុខសាយប័រនៅតែស្ថិតក្នុងដំណាក់កាលដំបូងនៃការអភិវឌ្ឍ។ កម្ពុជានៅមានភាព ខ្វះខាតនូវច្បាប់ទូទៅដែលគ្រប់គ្រងសន្តិសុខសាយប័រ និងការការពារទិន្នន័យ។ ជាលទ្ធផល មិន មានក្របខ័ណ្ឌច្បាប់ច្បាស់លាស់សម្រាប់ដោះស្រាយជាមួយឧក្រិដ្ឋកម្មតាមអ៊ីនធឺណិតនោះទេ ហើយយើងមិនមាននីតិវិធីស្តង់ដារណាមួយសម្រាប់ការរាយការណ៍អំពីឧប្បត្តិហេតុតាមអ៊ីនធឺណិត នោះឡើយ។ លើសពីនេះទៅទៀត កង្វះបទប្បញ្ញត្តិប្រកបដោយប្រសិទ្ធភាព និងការអនុវត្តសន្តិ សុខសាយប័រ បង្កើតបរិយាកាសប្រកួតប្រជែងសម្រាប់អាជីវកម្មដែលកំពុងប្រតិបត្តិការក្នុង ប្រទេសកម្ពុជា។ អវត្តមាននៃតម្រូវការបទប្បញ្ញត្តិ និងស្តង់ដារមានន័យថាអាជីវកម្មទាំងអស់ត្រូវ បានទុកចោលដើម្បីអភិវឌ្ឍគោលនយោបាយ និងការអនុវត្តសន្តិសុខសាយប័ររបស់ពួកគេ ដែល អាចបណ្តាលឱ្យខ្វះប្រសិទ្ធភាព និងភាពស៊ីសង្វាក់គ្នា។

ស្ថានភាពនយោបាយរបស់ប្រទេសកម្ពុជាកត្តាមួយទៀតដែលធ្វើឱ្យមានភាពស្មុគស្មាញដល់ បរិយាកាសសន្តិសុខសាយប័ររបស់ប្រទេស។ កម្ពុជាបានប្រឈមនឹងការចោទប្រកាន់ពីបទប្រើប្រា រកម្មតាមអ៊ីនធឺណិត ដើម្បីតាមដានឥស្សរជនគណបក្សប្រឆាំង អ្នកកាសែត និងក្រុមសង្គមស៊ីវិល។ ហេតុផលទាំងនេះបង្កើតបរិយាកាសលំបាកដល់ធុរកិច្ច និងបុគ្គលក្នុងប្រតិបត្តិការ ហើយវានឹងធ្វើ ឱ្យមានតម្រូវការសម្រាប់វិធានការសន្តិសុខសាយប័រកាន់តែខ្លាំង។

ដូច្នេះ សន្តិសុខសាយប័រ គឺជាបញ្ហាប្រឈមដ៏សំខាន់សម្រាប់ប្រទេសកម្ពុជា ហើយចាំបាច់ត្រូវមាន ការយល់ដឹងច្រើន ការវិនិយោគលើការអប់រំនិងការបណ្តុះបណ្តាល និងក្របខ័ណ្ឌបទប្បញ្ញត្តិដើម្បី កែលម្អការអនុវត្តសន្តិសុខសាយប័រ។ ជាមួយនឹងគោលនយោបាយ និងការអនុវត្តត្រឹមត្រូវ កម្ពុជា អាចកាត់បន្ថយហានិភ័យនៃការគំរាមកំហែងតាមអ៊ីនធឺណិត និងការពារប្រជាពលរដ្ឋ និងអាជីវកម្ម របស់ខ្លួនពីផលវិបាកអវិជ្ជមាននៃឧក្រិដ្ឋកម្មតាមអ៊ីនធឺណិត។ ខាងក្រោមនេះ គឺជាហេតុផល សំខាន់ៗដែលច្បាប់សន្តិសុខសាយប័រត្រូវការជាចាំបាច់ត្រូវកែសម្រួល។

១.៣. ភាពបន្ទាន់សម្រាប់តម្រូវការបន្ថែមនៃច្បាប់សន្តិសុខសាយបំរ

សន្តិសុខសាយបំរបានក្លាយទៅជាធាតុសំខាន់មួយនៅក្នុងក្របខ័ណ្ឌច្បាប់នៃប្រទេសនានាជុំវិញពិភពលោក ដោយសារស្ថាប័ន និងប្រព័ន្ធរបស់រដ្ឋាភិបាលមានព័ត៌មានរសើបយ៉ាងច្រើន ហើយការបំពានណាមួយនៃព័ត៌មាននេះអាចមានផលវិបាកធ្ងន់ធ្ងរដល់ សេដ្ឋកិច្ច ឬសន្តិសុខជាតិនៃប្រទេសនានា។ ដូច្នោះ ស្ថាប័នរដ្ឋាភិបាលមានទំនួលខុសត្រូវក្នុងការការពារព័ត៌មានផ្ទាល់ខ្លួនរបស់ប្រជាពលរដ្ឋ ការការពារអាចកំបាំងសន្តិសុខជាតិ និងធានាឱ្យមានដំណើរការយ៉ាងរលូននៃប្រតិបត្តិការរបស់រដ្ឋាភិបាល។

សន្តិសុខសាយបំរ គឺជារឿងចាំបាច់ដើម្បីការពារសន្តិសុខជាតិ (Tunggal, 2023)។ ស្ថាប័ន និងប្រព័ន្ធរបស់រដ្ឋាភិបាលមានព័ត៌មានជាច្រើនទាក់ទងនឹងសន្តិសុខជាតិ រួមទាំងអាចកំបាំងយោធាឯកសារដែល បានចាត់ថ្នាក់ និងទិន្នន័យសើបការណ៍។ ការវាយប្រហារតាមអ៊ីនធឺណិតលើប្រព័ន្ធរដ្ឋាភិបាលអាចធ្វើឱ្យព័ត៌មានរសើប ទាំងនេះ ទាញសន្តិសុខជាតិចូលទៅក្នុងហានិភ័យ។ លើសពីនេះ សន្តិសុខសាយបំរបានក្លាយជាភាពចាំបាច់ ដើម្បីធានា ដល់ប្រតិបត្តិការរបស់រដ្ឋាភិបាល។ ការវាយប្រហារតាមអ៊ីនធឺណិតទៅលើប្រព័ន្ធរបស់រដ្ឋាភិបាលអាចបណ្តាលឱ្យមានការរំខាន ដល់ប្រតិបត្តិការរបស់រដ្ឋាភិបាល ដូចជាអសមត្ថភាពក្នុងការដំណើរការការទូទាត់ ឬផ្តល់សេវាកម្មសំខាន់ៗជាដើម។ ការធានា ឱ្យមានដំណើរការរលូននៃប្រតិបត្តិការរបស់រដ្ឋាភិបាល មានសារៈសំខាន់ក្នុងការរក្សាស្ថិរភាពរបស់ប្រទេស។

ដូចដែលបានរៀបរាប់ខាងលើ ការអភិវឌ្ឍនៃវិស័យឌីជីថល និងហេដ្ឋារចនាសម្ព័ន្ធអ៊ីនធឺណិតបានបណ្តាលឱ្យមានការអភិវឌ្ឍ ជាវិជ្ជមាន និងមានបញ្ហាប្រឈមជាច្រើនផងដែរ ដូចជាការគំរាមកំហែងប្រឆាំងនឹងស្ថាប័នសាធារណៈដែលអាចប៉ះពាល់ដល់ ផ្នែកដ៏ធំមួយនៃចំនួនប្រជាជន ឬសង្គម។ ក្នុងបរិបទបែបនេះ ស្ថាប័នរដ្ឋាភិបាលមានទំនួលខុសត្រូវក្នុងការដោះស្រាយការគំរាមកំហែង តាមអ៊ីនធឺណិតដែលអាចប៉ះពាល់ដល់សង្គម។ វារួមបញ្ចូលទាំងការបង្កើតគោលនយោបាយ និងយុទ្ធសាស្ត្រដើម្បីការពារការវាយប្រហារតាមអ៊ីនធឺណិត ការកំណត់អត្តសញ្ញាណនៃការគំរាមកំហែងដែលអាចកើតមាន និងឆ្លើយតបយ៉ាងឆាប់រហ័សចំពោះឧបត្ថម្ភហេតុតាមអ៊ីនធឺណិតណាមួយ។ ការក្លែងបន្លំ គឺជាឧទាហរណ៍ជាក់លាក់មួយទៀត។ សន្តិសុខសាយបំរគឺចាំបាច់សម្រាប់ការការពារការក្លែងបន្លំ ជាពិសេសនៅក្នុងប្រព័ន្ធហិរញ្ញវត្ថុរបស់រដ្ឋាភិបាល។ ពួកឧក្រិដ្ឋជនតាមអ៊ីនធឺណិតអាចព្យាយាមចូលប្រើប្រព័ន្ធហិរញ្ញវត្ថុរបស់រដ្ឋាភិបាល ដើម្បីលួចលុយ ឬរៀបចំទិន្នន័យហិរញ្ញវត្ថុ ហើយវិធានការសន្តិសុខសាយបំរមានប្រសិទ្ធភាពគឺចាំបាច់ដើម្បីការពារការវាយប្រហារបែបនេះ។

ជាចុងក្រោយ សន្តិសុខសាយបំរ គឺត្រូវការជាចាំបាច់ដើម្បីរក្សាការជឿទុកចិត្តជាសាធារណៈ ដែលជាធាតុសំខាន់ដែល សិក្សាយ៉ាងទូលំទូលាយដោយអ្នកវិទ្យាសាស្ត្រនយោបាយ (Levi and Stoker, 2020)។ នៅពេលដែលមនុស្សចែករំលែក ព័ត៌មានផ្ទាល់ខ្លួនរបស់ពួកគេជាមួយស្ថាប័នរដ្ឋាភិបាល ពួកគេរំពឹងថាទិន្នន័យរបស់ពួកគេនឹងត្រូវបានរក្សាទុកដោយសុវត្ថិភាព។ រាល់ការ

បំពានលើការដើរទុកចិត្តនេះអាចបំផ្លាញទំនុកចិត្តសាធារណៈនៅក្នុងស្ថាប័នរដ្ឋាភិបាល និងធ្វើឱ្យខូចដល់ភាពស្របច្បាប់ នៃសកម្មភាពរបស់រដ្ឋាភិបាល។

ដូចឧទាហរណ៍ខាងលើ សន្តិសុខសាយបំរែមានសារៈសំខាន់ណាស់សម្រាប់ស្ថាប័ន និងប្រព័ន្ធរបស់រដ្ឋាភិបាលដើម្បី ការពារព័ត៌មានរសើប រក្សាការដើរទុកចិត្តសាធារណៈ ធានាប្រតិបត្តិការរបស់រដ្ឋាភិបាល ការពារការក្លែងបន្លំ និងដោះស្រាយ ការគំរាមកំហែងតាមអ៊ីនធឺណិត។ ការបង្កើតយុទ្ធសាស្ត្រសន្តិសុខសាយបំរែដ៏រឹងមាំនាពេលបច្ចុប្បន្ននេះ គឺមានភាពចាំបាច់ ជាងពេលមុនដោយសារការពន្លឿនឌីជីថលភាវូបនីយកម្ម និងការគំរាមកំហែងកាន់តែខ្លាំងឡើងទៅលើអ៊ីនធឺណិត (ASEAN, 2022) ដែលបានក្លាយជាបញ្ហាឆ្លងព្រំដែនដែលទាមទារកិច្ចសហប្រតិបត្តិការក្នុងតំបន់។ ដើម្បីប្រឈមមុខនឹងការគំរាម កំហែងទាំងនេះ និងលើកកម្ពស់កិច្ចសហប្រតិបត្តិការក្នុងចំណោមប្រជាជាតិអាស៊ីអាគ្នេយ៍អាស៊ានបានបង្កើត យុទ្ធសាស្ត្រកិច្ចសហប្រតិបត្តិការសន្តិសុខសាយបំរែអាស៊ាន ឆ្នាំ២០២១-២០១៥ (ដូចឯកសារយោងខាងដើម)។ សសរស្តម្ភទាំងប្រាំមានគោលបំណងដូចជា (១) ការត្រៀមខ្លួនរួចជាស្រេចក្នុងការជំរុញកិច្ចសហប្រតិបត្តិការតាមអ៊ីនធឺណិត (២) ការពង្រឹងការសម្របសម្រួលគោលនយោបាយអ៊ីនធឺណិតក្នុងតំបន់ (៣) ការបង្កើនទំនុកចិត្តលើអ៊ីនធឺណិត (៤) [ការបង្កើត] ការកសាងសមត្ថភាពក្នុងតំបន់ និង (៥) [ការលើកកម្ពស់] កិច្ចសហប្រតិបត្តិការអន្តរជាតិ។ ដូច្នេះហើយ កិច្ចខិតខំប្រឹងប្រែងរបស់កម្ពុជាក្នុងការពង្រឹងសន្តិសុខសាយបំរែរបស់ខ្លួន មិនត្រឹមតែជាភាពចាំបាច់ដើម្បីកែលម្អសុវត្ថិភាពនៅក្នុងវិស័យឌីជីថលកម្ពុជាប៉ុណ្ណោះទេ វាក៏ជាការរួមចំណែក ជាវិជ្ជមានដល់កិច្ចខិតខំប្រឹងប្រែងរួមដែលធ្វើឡើងដោយអាស៊ាន ដើម្បីដោះស្រាយបញ្ហាសន្តិសុខសាយបំរែជាសកល។

តាមរយៈការវិនិយោគលើវិធានការសន្តិសុខសាយបំរែប្រកបដោយប្រសិទ្ធភាព ស្ថាប័នរដ្ឋាភិបាលអាចជួយកាត់បន្ថយហានិភ័យ នៃការវាយប្រហារតាមអ៊ីនធឺណិត និងធានាសុវត្ថិភាព និងសន្តិសុខរបស់ប្រទេស។ ឯកសារទាំងអស់ខាងក្រោមនេះនឹងវាយតម្លៃការវិវឌ្ឍផ្នែកសន្តិសុខសាយបំរែរបស់កម្ពុជាដើម្បីបង្ហាញថា ទោះបីជាប្រទេសកម្ពុជាមានវឌ្ឍនភាពគួរឱ្យកត់សម្គាល់ក្នុងការអភិវឌ្ឍច្បាប់សន្តិសុខសាយបំរែក៏ដោយ ក៏បទប្បញ្ញត្តិច្បាប់ចាំបាច់ត្រូវមានការកែកុនបន្ថែមទៀត ដោយត្រូវមានធាតុចូលពី ភ្នាក់ងារសង្គមស៊ីវិលផ្សេងៗ ដូច្នេះច្បាប់ថ្មីមានលក្ខណៈជាសិទ្ធិសេរីភាព និងបរិយាបន្នហើយវាក៏រួមចំណែកបន្ថែមទៀត ដល់ការអភិវឌ្ឍប្រកបដោយចីរភាពរបស់ប្រទេសផងដែរ។

២. ច្បាប់សន្តិសុខសាយបំរែ

បើប្រៀបធៀបទៅនឹងប្រភេទច្បាប់ផ្សេងទៀត ឧក្រិដ្ឋកម្មតាមអ៊ីនធឺណិតត្រូវការ ការពិនិត្យ និងអភិវឌ្ឍផ្លូវច្បាប់បន្ថែមទៀត។ ទោះជាយ៉ាងណាក៏ដោយ វាត្រូវតែមាននៅក្នុងក្របខ័ណ្ឌច្បាប់ក្នុងប្រទេស (Corrado និង សកល, ២០២១)។ បទល្មើសទាក់ទងនឹងកុំព្យូទ័រត្រូវបានដាក់បញ្ចូលរួចជាស្រេចនៅក្នុងក្រមព្រហ្មទណ្ឌ (ឆ្នាំ២០០៩) ក្នុងមាត្រា ៣១៧ ដល់ ៣២០ និង មាត្រា ៤២៧ ដល់ ៤៣២។ ទោះជាយ៉ាងណាក៏ដោយ ច្បាប់ទាំងនេះមានភាពមិនច្បាស់លាស់ ហើយដោយសារតែការអភិវឌ្ឍយ៉ាងឆាប់រហ័សនៃលំហឌីជីថលនៅក្នុងប្រទេស ច្បាប់នេះដើរមិនទាន់សម័យកាល។

អាស្រ័យហេតុនេះ ក្នុងទសវត្សរ៍ចុងក្រោយនេះប្រទេសកម្ពុជាបានអនុម័តច្បាប់ និងបទប្បញ្ញត្តិ មួយចំនួនទាក់ទងនឹង សន្តិសុខសាយបំរើ ដើម្បីការពារប្រជាពលរដ្ឋ វិស័យធុរកិច្ច និងហេដ្ឋារចនា សម្ព័ន្ធសំខាន់ៗពីការគំរាមកំហែងតាមអ៊ីនធឺណិត។ សរុបមក វាតំណាងឱ្យវឌ្ឍនភាពដ៏មាន អត្ថន័យឆ្ពោះទៅរកការបង្កើត និងការបង្រួបបង្រួមក្របខ័ណ្ឌបទប្បញ្ញត្តិនៃវិស័យ ឌីជីថលនៅ កម្ពុជា។ ទោះបីជាមានការវិវឌ្ឍដែលត្រូវបានធ្វើឡើងជាមួយនឹងការបង្កើតបទប្បញ្ញត្តិច្បាប់ថ្មី ក៏ដោយ អត្ថបទនេះក៏នឹងបង្ហាញផងដែរថា បទប្បញ្ញត្តិផ្លូវច្បាប់ដែលបានបង្កើតឡើងដើម្បីដោះ ស្រាយបញ្ហាប្រឈមនៃវិស័យឌីជីថល ត្រូវតែត្រូវបានអភិវឌ្ឍបន្ថែមទៀត ដូច្នោះវានឹងកាន់តែមាន បរិយាបន្ន ខណៈពេលដែលកំពុងពិចារណាទៅលើទស្សនៈនិងតម្រូវការរបស់គ្រប់ភាគីពាក់ព័ន្ធ របស់សង្គមស៊ីវិល។ ខាងក្រោមនេះ ច្បាប់ស្តីពីឧក្រិដ្ឋកម្មតាមអ៊ីនធឺណិតទាំងប្រាំដែលត្រូវបាន ពិនិត្យ៖ ច្បាប់ស្តីពីការគ្រប់គ្រងវិស័យទូរគមនាគមន៍ជាតិ ច្បាប់ស្តីពីឧក្រិដ្ឋកម្មតាមអ៊ីនធឺណិត អនុក្រឹត្យ ស្តីពីការបង្កើតអាជ្ញាធរជាតិប្រយុទ្ធប្រឆាំងនឹងឧក្រិដ្ឋកម្មតាមអ៊ីនធឺណិត ប្រកាសស្តីពីការ គ្រប់គ្រងសន្តិសុខសាយបំរើ និងអនុក្រឹត្យស្តីពីការបង្កើតគណៈកម្មាធិការជាតិសន្តិសុខសាយបំរើ។ ច្បាប់ទាំងប្រាំនេះត្រូវបានត្រួតពិនិត្យមើលដោយផ្នែកកទៅលើវឌ្ឍនភាពរបស់វា។ បន្ទាប់មក បញ្ហា ប្រឈមដែលពាក់ព័ន្ធនៃច្បាប់ទាំងនោះនឹងត្រូវបានបង្ហាញ។ ការណ៍នេះនឹងអនុញ្ញាតឱ្យការវិភាគ បាននូវអ្វីដែលបទប្បញ្ញត្តិទាក់ទងនឹងឧក្រិដ្ឋកម្មតាមអ៊ីនធឺណិតមានដូចគ្នាជាមួយ និងបង្ហាញអំពី របៀបពង្រឹងច្បាប់ទាំងនេះនៅក្នុងផ្នែកទី៣។

២.១. ច្បាប់ស្តីពីការគ្រប់គ្រងវិស័យទូរគមនាគមន៍ជាតិ

ច្បាប់ស្តីពីការគ្រប់គ្រងវិស័យទូរគមនាគមន៍ជាតិ (អង្គការពាណិជ្ជកម្មពិភពលោក, n.d) ត្រូវបាន អនុម័តនៅឆ្នាំ ២០១៥។ ច្បាប់នេះគ្របដណ្តប់ទៅលើការគ្រប់គ្រង និងបទប្បញ្ញត្តិនៃវិស័យ ទូរគមនាគមន៍របស់ប្រទេស រួមទាំងបញ្ហាទាក់ទងនឹងសន្តិសុខសាយបំរើផងដែរ។ ច្បាប់នេះ បង្ហាញពីបទប្បញ្ញត្តិសំខាន់ៗមួយចំនួនដូចជា ការបង្កើតនិយ័តករទូរគមនាគមន៍កម្ពុជា (TRC) ដែលជាស្ថាប័នគ្រប់គ្រង ទទួលខុសត្រូវក្នុងការត្រួតពិនិត្យវិស័យទូរគមនាគមន៍នៅកម្ពុជា។ វាក៏ មានច្បាប់គ្រប់គ្រងទៅលើការ តម្រូវឱ្យមានអាជ្ញាប័ណ្ណផងដែរ។ ច្បាប់នេះកំណត់ពីតម្រូវឱ្យមាន អាជ្ញាប័ណ្ណសម្រាប់អ្នកផ្តល់សេវាទូរគមនាគមន៍នៅកម្ពុជា រួមទាំងតម្រូវការដើម្បីទទួលបានអាជ្ញា ប័ណ្ណពី TRC មុនពេលផ្តល់សេវាទូរគមនាគមន៍។ ការគ្រប់គ្រងវិសាលគមក៏រងផល ប៉ះពាល់ ដោយច្បាប់ស្តីពីការគ្រប់គ្រងវិស័យទូរគមនាគមន៍របស់ប្រទេសផងដែរ។ ច្បាប់គ្រប់គ្រង ការបែងចែក និងការគ្រប់គ្រងប្រេកង់វិទ្យុ និងទម្រង់ផ្សេងទៀតនៃវិសាលគមដែលប្រើសម្រាប់សេវា ទូរគមនាគមន៍។ ច្បាប់នេះក៏ទាក់ទងនឹង កាតព្វកិច្ចសេវាកម្មជាសកលផងដែរ។ វាបង្កើតកាតព្វកិច្ច សេវាកម្មជាសកលសម្រាប់អ្នកផ្តល់សេវាទូរគមនាគមន៍ដោយតម្រូវឱ្យ ពួកគេផ្តល់សេវា ទូរគមនាគមន៍ដែលមានតម្លៃសមរម្យ និងអាចប្រើប្រាស់បានដល់ប្រជាពលរដ្ឋកម្ពុជាទាំងអស់ ដោយមិនគិតពី ទីតាំង ឬស្ថានភាពសេដ្ឋកិច្ចរបស់ពួកគេ។ ចំណុចចុងក្រោយ វាក៏ចង្អុលបង្ហាញពី បញ្ហាសន្តិសុខសាយបំរើដោយខ្លួនឯងជាមួយនឹង បទប្បញ្ញត្តិទាក់ទងនឹងសន្តិសុខសាយបំរើដែល តម្រូវឱ្យអ្នកផ្តល់សេវាទូរគមនាគមន៍អនុវត្តវិធានការសុវត្ថិភាពសមស្របដើម្បីការពារបណ្តាញ និង ប្រព័ន្ធរបស់ពួកគេពីការគំរាមកំហែងតាមអ៊ីនធឺណិត។ សរុបសេចក្តី ច្បាប់ស្តីពីការគ្រប់គ្រងវិស័យ

ទូរគមនាគមន៍ជាតិ មានគោលបំណងជំរុញការអភិវឌ្ឍវិស័យទូរគមនាគមន៍ប្រកបដោយភាព
ប្រកួតប្រជែង និងប្រកបដោយភាព ច្នៃប្រឌិតនៅកម្ពុជា ហើយក៏ធានាថាវិស័យនេះដំណើរការ
ដោយយុត្តិធម៌ តម្លាភាព និងសុវត្ថិភាព។

ខណៈដែលច្បាប់ស្តីពីការគ្រប់គ្រងវិស័យទូរគមនាគមន៍ជាតិនៅកម្ពុជាទទួលបានការកោតសរសើរ
ចំពោះការខិតខំប្រឹងប្រែងរបស់ខ្លួន ក្នុងការលើកកម្ពស់ការអភិវឌ្ឍវិស័យទូរគមនាគមន៍
ប្រកបដោយភាពប្រកួតប្រជែង និងប្រកបដោយភាពច្នៃប្រឌិតនោះ ក៏មានការរិះគន់មួយចំនួន
ទៅលើច្បាប់នេះផងដែរ។ អ្នករិះគន់ (អង្គការឃ្លាំមើលសិទ្ធិមនុស្ស, ២០២១) បានអះអាងថា
ច្បាប់នេះមិនមានភាពច្បាស់លាស់គ្រប់គ្រាន់ ឬជាក់លាក់នៅក្នុងបទប្បញ្ញត្តិរបស់ខ្លួននោះទេ ជា
ពិសេសនៅពេលដែលនិយាយអំពីបញ្ហាទាក់ទងទៅនឹងសន្តិសុខសាយបរ។

កង្វះភាពច្បាស់លាស់នេះអាចនាំឱ្យមានភាពមិនស៊ីសង្វាក់គ្នាក្នុងការអនុវត្ត និងការពង្រឹងច្បាប់
(សេង, ២០២២)។ ការព្រួយបារម្ភមួយទៀតដែលទាក់ទងនឹងច្បាប់នេះ គឺការប្រកួតប្រជែងនៅ
មានកម្រិត។ អ្នកសង្កេតការណ៍មួយចំនួន បានលើកឡើងពីការព្រួយបារម្ភថា ច្បាប់នេះធ្វើមិនបាន
គ្រប់គ្រាន់ ដើម្បីលើកកម្ពស់ការប្រកួតប្រជែងក្នុងវិស័យទូរគមនាគមន៍នោះទេ។ ការព្រួយបារម្ភ
ទៅលើតម្រូវការឱ្យមានអាជ្ញាប័ណ្ណ និងបទប្បញ្ញត្តិផ្សេងទៀតអាចបង្កការលំបាកសម្រាប់អ្នកផ្តល់
សេវាកម្មថ្មីៗដើម្បីប្រលូកនៅក្នុងទីផ្សារ។ ដូចគ្នានេះដែរ ភាពនៅមានកម្រិតនៃការការពារអ្នកប្រើ
ប្រាស់ក៏បានលើកឡើងជាការព្រួយបារម្ភមួយផងដែរ ដោយសារច្បាប់នេះធ្វើមិនបានគ្រប់គ្រាន់ក្នុង
ការការពារសិទ្ធិ និងផលប្រយោជន៍របស់អ្នកប្រើប្រាស់នោះទេ។ ជាឧទាហរណ៍ អ្នករិះគន់ខ្លះ
អះអាងថា ច្បាប់នេះមិនបានដោះស្រាយបញ្ហាឱ្យបានគ្រប់គ្រាន់ ដូចជាគុណភាពនៃសេវាកម្ម តម្លៃ
និងលទ្ធភាពប្រើប្រាស់។ ចំណុចចុងក្រោយ កង្វះការអនុវត្ត គឺជាចំណុចសំខាន់មួយទៀតដែល
ត្រូវយកចិត្តទុកដាក់។ អ្នករិះគន់ក៏បានកត់សម្គាល់ផងដែរថា ច្បាប់នេះប្រហែលជាមិនត្រូវបាន
អនុវត្តប្រកបដោយប្រសិទ្ធភាពទេ ជាពិសេសនៅតំបន់ជនបទ និងតំបន់ជាប់ស្រយាលនៃប្រទេស
ដែលលទ្ធភាពទទួលបានសេវាទូរគមនាគមន៍នៅមានកម្រិត។

សរុបមក ខណៈពេលដែលច្បាប់ស្តីពីការគ្រប់គ្រងវិស័យទូរគមនាគមន៍ជាតិតំណាងឱ្យការបោះ
ជំហានទៅមុខដ៏សំខាន់ក្នុងការអភិវឌ្ឍវិស័យទូរគមនាគមន៍របស់កម្ពុជានោះ វាក៏មានការព្រួយ
បារម្ភថាច្បាប់នេះប្រហែលជាត្រូវកែសម្រួល និងកែលម្អដើម្បី ដោះស្រាយការរិះគន់ទាំងនេះ និង
ការរិះគន់ផ្សេងទៀត។

២.២. ច្បាប់ស្តីពីឧក្រិដ្ឋកម្មតាមអ៊ីនធឺណិត

ច្បាប់ស្តីពីឧក្រិដ្ឋកម្មតាមអ៊ីនធឺណិត (អូឌីស៊ីប, n.d) នៅកម្ពុជាត្រូវបានព្រាងនៅឆ្នាំ ២០១៨
ដើម្បីដោះស្រាយការគំរាមកំហែងកាន់តែខ្លាំងឡើងនៃឧក្រិដ្ឋកម្មតាមអ៊ីនធឺណិតនៅក្នុងប្រទេស។
ច្បាប់នេះធ្វើការផ្តន្ទាទោសលើសកម្មភាពតាមអ៊ីនធឺណិតជាច្រើន និងផ្តល់ក្របខ័ណ្ឌច្បាប់សម្រាប់
ការស៊ើបអង្កេត និងកាត់ទោសករណីឧក្រិដ្ឋកម្មតាមអ៊ីនធឺណិត។ ច្បាប់នេះមានសារៈសំខាន់ដោយ
សារវាបង្កើតគោលគំនិតសំខាន់ៗ។ ឧក្រិដ្ឋកម្មតាមអ៊ីនធឺណិតត្រូវបានកំណត់ថាជាបទល្មើស

ព្រហ្មទណ្ឌណាមួយដែលបាន ប្រព្រឹត្តដោយប្រើប្រព័ន្ធបច្ចេកវិទ្យាព័ត៌មាន និងទំនាក់ទំនង (ICT) រួមទាំងការលួចចូល ការបន្លំ ការលួចអត្តសញ្ញាណ និងការ ចែកចាយមេរោគ។ ដូច្នោះហើយវាក៏ បង្កើតការពិន័យដែលពាក់ព័ន្ធផងដែរ។ ច្បាប់នេះដាក់ទោសទណ្ឌចំពោះបទល្មើស តាមអ៊ីនធឺណិត រាប់ចាប់ពីការដាក់ពិន័យរហូតដល់ដាក់ពន្ធនាគារ។ ឧទាហរណ៍ ការពិន័យស្រាលបំផុតចំពោះការ ចូលប្រើ ប្រព័ន្ធកុំព្យូទ័រដោយគ្មានការអនុញ្ញាតគឺត្រូវជាប់ពន្ធនាគារ ៣ឆ្នាំ និងពិន័យជាប្រាក់រហូត ដល់ ១០លានរៀល (២.៥០០ ដុល្លារ អាមេរិក) (ណារិន, ២០២២)។

ប្រសិនបើច្បាប់នេះត្រូវបានអនុម័ត តុលាការកម្ពុជាអាចអនុវត្តយុត្តាធិការក្រៅទឹកដីប្រទេស កម្ពុជាលើឧក្រិដ្ឋកម្មតាមអ៊ីនធឺណិត ដែលបានប្រព្រឹត្តនៅក្រៅប្រទេសកម្ពុជា បើបទល្មើ សមានផលប៉ះពាល់ដល់ប្រទេសកម្ពុជា ឬពាក់ព័ន្ធនឹងសញ្ជាតិខ្មែរ (Kellihier, ២០២៣)។ ក្នុង ករណីចាំបាច់ ច្បាប់នេះនឹងផ្តល់ការស៊ើបអង្កេត និងកាត់ទោសឧក្រិដ្ឋកម្មតាមអ៊ីនធឺណិត ដោយ ប៉ូលីស និងតុលាការ។ វាក៏បង្កើតនីតិវិធីសម្រាប់ការប្រមូល និងការទទួលយក ភស្តុតាងអេឡិចត្រូនិកនៅក្នុងករណីឧក្រិដ្ឋ កម្មតាមអ៊ីនធឺណិតផងដែរ។ ច្បាប់នេះរួម បញ្ចូលបទប្បញ្ញត្តិ ដើម្បីការពារសិទ្ធិជនរងគ្រោះ និងសាក្សីនៃឧក្រិដ្ឋកម្មតាមអ៊ីនធឺណិត រួមទាំង សិទ្ធិឯកជនភាព ការសម្ងាត់ និងការការពារពីការសងសឹក។

ខណៈពេលដែលច្បាប់ស្តីពីឧក្រិដ្ឋកម្មតាមអ៊ីនធឺណិតនៅកម្ពុជាគឺជាជំហានដ៏សំខាន់មួយឆ្ពោះ ទៅមុខក្នុងការដោះស្រាយឧក្រិដ្ឋកម្មតាមអ៊ីនធឺណិតនៅក្នុងប្រទេសនោះ មានមតិវិះគន់មួយចំនួន ចំពោះច្បាប់នេះ។ ច្បាប់នេះត្រូវបានគេវិះគន់ដោយសារតែវាមិនសូវជាមានភាពច្បាស់លាស់ និង ទូលំទូលាយពេក ដែលទុកឱកាសឱ្យមានការបកប្រែ និងការបំពានដែលអាចកើតមាន។ វាអាចនាំ ឱ្យមានការផ្តោតទៅដល់អ្នកប្រឆាំងនយោបាយ សកម្មជនសិទ្ធិមនុស្ស និងបុគ្គលផ្សេងទៀតដែល បញ្ចេញមតិមិនពេញចិត្តតាមអ៊ីនធឺណិត។ ភាពខ្វះខាតនៃដំណើរការត្រឹមត្រូវក៏គួរតែត្រូវបាន បញ្ជាក់ផងដែរ (ដូចឯកសារយោងខាងដើម)។ អ្នកសង្កេតការណ៍មួយចំនួនបានលើកឡើងពីការ ព្រួយបារម្ភថា ច្បាប់នេះមិនផ្តល់ឱ្យបានគ្រប់គ្រាន់នូវដំណើរការនៃការ ការពារសម្រាប់បុគ្គលដែល ត្រូវបានចោទប្រកាន់ពីបទឧក្រិដ្ឋកម្មតាមអ៊ីនធឺណិត។ ឧទាហរណ៍ ច្បាប់នេះអនុញ្ញាតឱ្យមាន ការឃុំខ្លួនបណ្តោះអាសន្នរហូតដល់ប្រាំមួយខែ ដែលអ្នកខ្លះប្រកែកថាហួសហេតុ។ ការខ្វះខាត ច្បាស់លាស់របស់ខ្លួនលើភស្តុតាង អេឡិចត្រូនិក គឺជាបញ្ហាមួយទៀតដែលបង្ហាញថា វានៅតែ មានកន្លែងសម្រាប់ធ្វើឱ្យប្រសើរឡើងនៅក្នុងក្របខ័ណ្ឌច្បាប់សន្តិសុខសាយប័ររបស់កម្ពុជា។ មាន ការព្រួយបារម្ភដែលថា ច្បាប់នេះមិនផ្តល់ការណែនាំច្បាស់លាស់អំពីលទ្ធភាពទទួលយកបាន និង ភាពជឿជាក់នៃភស្តុតាងអេឡិចត្រូនិកនៅក្នុងករណី ឧក្រិដ្ឋកម្មតាមអ៊ីនធឺណិត។ វាអាចនាំឱ្យមាន ភាពមិនស៊ីសង្វាក់គ្នាក្នុងការអនុវត្តច្បាប់ និងធ្វើឱ្យប៉ះពាល់ដល់ភាពយុត្តិធម៌នៃការ កាត់ក្តី។ ជា ចុងក្រោយ ផលប៉ះពាល់ដែលមានសក្តានុពលទៅលើសេរីភាពនៃការបញ្ចេញមតិ មិនគួរត្រូវបាន មើលរំលងឡើយ (វិទ្យាស្ថានសារព័ត៌មានអន្តរជាតិ, ២០២០)។ មានការព្រួយបារម្ភថាច្បាប់នេះ អាចត្រូវបានប្រើប្រាស់ ដើម្បីរារាំងការបញ្ចេញមតិដោយសេរី និងការមិនយល់ស្រប ជាពិសេសត្រូវ បានផ្តល់និយមន័យទូលំទូលាយនៃបទល្មើសឧក្រិដ្ឋកម្មតាមអ៊ីនធឺណិត។ អ្នកវិះគន់មួយចំនួនបាន លើកឡើងថា ច្បាប់នេះអាចត្រូវបានប្រើ ដើម្បីកំណត់គោលដៅលើអ្នកកាសែត សកម្មជនសិទ្ធិ មនុស្ស និងឥស្សរជនគណបក្សប្រឆាំង ដែលប្រើប្រព័ន្ធអ៊ីនធឺណិត ដើម្បីបញ្ចេញមតិរបស់ពួកគេ។

ករណីខាងលើបង្ហាញពីជំហានវិជ្ជមានដ៏មានអត្ថន័យឆ្ពោះទៅរកបទប្បញ្ញត្តិនៃលំហដីដីថល។ ទោះយ៉ាងណាក៏ដោយ ក៏នៅតែមានការព្រួយបារម្ភថា ច្បាប់នេះអាចនឹងត្រូវកែប្រែនិងធ្វើឱ្យប្រសើរ ឡើង ដើម្បីដោះស្រាយការរិះគន់ទាំងនេះ និងការរិះគន់ផ្សេងទៀត ដែលមិនត្រូវមើលរំលង។ វា មានសារៈសំខាន់ណាស់ក្នុងការធ្វើឱ្យមានតុល្យភាពរវាងការការពារ ប្រជាពលរដ្ឋពីការគំរាមកំហែង តាមអ៊ីនធឺណិត និងការការពារសិទ្ធិ និងសេរីភាពជាមូលដ្ឋានរបស់ពួកគេ។

២.៣. អនុក្រឹត្យស្តីពីការបង្កើតអាជ្ញាធរជាតិប្រយុទ្ធប្រឆាំង នឹងឧក្រិដ្ឋកម្មតាមអ៊ីនធឺណិត

អនុក្រឹត្យ (មាត្រា១៩, n.d) នេះត្រូវបានដាក់ចេញក្នុងឆ្នាំ២០១៤ ដើម្បីពង្រឹងកិច្ចខិតខំប្រឹងប្រែង របស់ប្រទេសក្នុង ការប្រយុទ្ធប្រឆាំងនឹងឧក្រិដ្ឋកម្មតាមអ៊ីនធឺណិត។ វារៀបរាប់អំពីមុខងារ និងការ ទទួលខុសត្រូវរបស់អាជ្ញាធរជាតិ ប្រយុទ្ធប្រឆាំងនឹងឧក្រិដ្ឋកម្មតាមអ៊ីនធឺណិត (NACC) និងផ្តល់ នូវក្របខ័ណ្ឌច្បាប់សម្រាប់ប្រតិបត្តិការរបស់ខ្លួន។ បទប្បញ្ញត្តិសំខាន់ៗមួយចំនួននៃអនុក្រឹត្យមាន ដូចតទៅ។ អាជ្ញាធរជាតិប្រយុទ្ធប្រឆាំងនឹងឧក្រិដ្ឋកម្មតាមអ៊ីនធឺណិត ជាអាជ្ញាធរជាតិទទួលបន្ទុក ប្រយុទ្ធប្រឆាំងឧក្រិដ្ឋកម្មតាមអ៊ីនធឺណិតនៅកម្ពុជា។ ស្ថាប័ននេះក៏ទទួលបន្ទុកលើការបង្កើតគោល នយោបាយ យុទ្ធសាស្ត្រ និងផែនការសម្រាប់ទប់ស្កាត់ និងប្រយុទ្ធប្រឆាំងនឹងឧក្រិដ្ឋកម្ម តាមអ៊ីនធឺណិត ក៏ដូចជាការសម្របសម្រួល និងសហប្រតិបត្តិការជាមួយទីភ្នាក់ងាររដ្ឋាភិបាល ផ្សេងទៀត អង្គការសង្គមស៊ីវិល និងដៃគូអន្តរជាតិ។ សមាសភាពរបស់ អាជ្ញាធរជាតិប្រយុទ្ធ ប្រឆាំងនឹងឧក្រិដ្ឋកម្មតាមអ៊ីនធឺណិតរួមមានតំណាងមកពីស្ថាប័នរដ្ឋាភិបាលផ្សេងៗ ដែលមាន ក្រសួងមហាផ្ទៃ ក្រសួងប្រៃសណីយ៍ និងទូរគមនាគមន៍ ក្រសួងយុត្តិធម៌ និងក្រសួងព័ត៌មាន។

អាជ្ញាធរជាតិនេះមានអំណាចក្នុងការស៊ើបអង្កេត ប្រមូល និងវិភាគទិន្នន័យដែលទាក់ទងនឹងឧក្រិដ្ឋ កម្មតាមអ៊ីនធឺណិត ផ្តល់ជំនួយ បច្ចេកទេស និងការកសាងសមត្ថភាពដល់ភ្នាក់ងារ និងអ្នកពាក់ ព័ន្ធផ្សេងទៀត ព្រមទាំងលើកកម្ពស់ការយល់ដឹងជាសាធារណៈ និងការអប់រំអំពីបញ្ហាឧក្រិដ្ឋកម្ម តាមអ៊ីនធឺណិត។ លើសពីនេះ អនុក្រឹត្យនេះផ្តល់ការបែងចែកថវិកានិងធនធានសម្រាប់ ប្រតិបត្តិ ការរបស់អាជ្ញាធរនេះរួមទាំងការបង្កើតអង្គការស៊ើបអង្កេតឧក្រិដ្ឋកម្មតាមអ៊ីនធឺណិតនៅក្នុងអគ្គ ស្នងការនគរបាលជាតិ។

សរុបមក អនុក្រឹត្យស្តីពីការបង្កើតអាជ្ញាធរជាតិប្រយុទ្ធប្រឆាំងនឹងឧក្រិដ្ឋកម្មតាមអ៊ីនធឺណិតនៅ កម្ពុជានេះ មានអត្ថន័យ ដោយសារវាគិតគូរអំពីការបង្កើតអាជ្ញាធរជាតិដែលយកចិត្តទុកដាក់ ផ្តល់ ក្របខ័ណ្ឌច្បាប់សម្រាប់ប្រតិបត្តិការរបស់ខ្លួន និងជួយ ធានាថាឧក្រិដ្ឋកម្មតាមអ៊ីនធឺណិតត្រូវ បានយកចិត្តទុកដាក់យ៉ាងខ្លាំង ដូច្នេះរដ្ឋាភិបាលអាចបង្កើតឧបករណ៍ និងធនធានដែល ខ្លួនត្រូវ ការ ដើម្បីដោះស្រាយការគំរាមកំហែងដែលកំពុងកើនឡើងនេះប្រកបដោយប្រសិទ្ធភាព។ ទោះបី យ៉ាងណា អនុក្រឹត្យនេះមិនបានគេចផុតពីការរិះគន់នោះទេ។ អ្នករិះគន់បានលើកឡើងពីការ ព្រួយបារម្ភថា អាជ្ញាធរជាតិនេះមិនមានតម្លាភាព ក្នុងដំណើរការបង្កើត ការសម្រេចចិត្ត និង សកម្មភាពរបស់ខ្លួន។ វាអាចនាំឱ្យមានសំណួរអំពីភាពស្របច្បាប់ និងតម្លាភាព របស់អាជ្ញាធរជាតិ និងសកម្មភាពរបស់ខ្លួន។ អនុក្រឹត្យនេះក៏ត្រូវបានរិះគន់ផងដែរ ទៅលើកង្វះខាតនៃឯករាជ្យភាពពី

រដ្ឋាភិបាល ដែលអាចកំណត់សមត្ថភាពរបស់ខ្លួនក្នុងការស៊ើបអង្កេត និងកាត់ទោសករណីឧក្រិដ្ឋ កម្មតាមអ៊ីនធឺណិតប្រកបដោយ ប្រសិទ្ធភាព។ វាក៏អាចនាំឱ្យមានសំណួរអំពីភាពមិនលំអៀង និង យុត្តិធម៌របស់អាជ្ញាធរជាតិប្រយុទ្ធប្រឆាំងនឹងឧក្រិដ្ឋកម្មតាមអ៊ីនធឺណិតផងដែរ។

ការព្រួយបារម្ភផ្សេងទៀតទាក់ទងនឹងការខ្វះខាតច្បាប់លាស់របស់ខ្លួនលើយុត្តាធិការ ដោយ ហេតុថាអនុក្រឹត្យនេះ មិនបានផ្តល់នូវការណែនាំច្បាស់លាស់អំពីយុត្តាធិការ និងវិសាលភាពនៃ សិទ្ធិអំណាចរបស់ អាជ្ញាធរជាតិប្រយុទ្ធប្រឆាំងនឹងឧក្រិដ្ឋកម្មតាមអ៊ីនធឺណិតដែលអាចនាំឱ្យមាន ភាពមិនស៊ីសង្វាក់ក្នុងការអនុវត្តច្បាប់ និងធ្វើឱ្យប៉ះពាល់ដល់ភាពយុត្តិធម៌នៃការជំនុំជម្រះ។ ដូច គ្នាទៅនឹងច្បាប់ស្តីពីឧក្រិដ្ឋកម្មតាមអ៊ីនធឺណិតដែរ អនុក្រឹត្យនេះក៏អាចនឹងមានផលប៉ះពាល់ដល់ សេរីភាពនៃការបញ្ចេញមតិផងដែរ ព្រោះវាអាចត្រូវបាន ប្រើដើម្បីរារាំងការបញ្ចេញមតិដោយសេរី និងគំនិតមិនយល់ស្រប ដោយសារតែនិយមន័យដ៏ទូលំទូលាយនៃបទល្មើសតាមអ៊ីនធឺណិត។ អ្នករិះគន់ខ្លះអះអាងថា អនុក្រឹត្យនេះអាចប្រើ ដើម្បីកំណត់គោលដៅអ្នកកាសែត សកម្មជនសិទ្ធិ មនុស្ស និងឥស្សរជនគណបក្សប្រឆាំងដែលប្រើវេទិកាអនឡាញ ដើម្បីបញ្ចេញទស្សនៈរបស់ ពួកគេ។

ដូច្នេះការវាយតម្លៃជាមួយនៃអនុក្រឹត្យនេះគឺស្របតាមបទប្បញ្ញត្តិច្បាប់ពីមុនចំនួនពីរ។ ខណៈពេល ដែលវាអាចត្រូវបានគេយល់ថា ជាការអភិវឌ្ឍន៍ជាវិជ្ជមានសម្រាប់ប្រទេសនេះ វាក៏នៅតែមាន កន្លែងសម្រាប់ការកែលម្អ ដើម្បីពង្រឹងបន្ថែម នឹងដោះស្រាយការរិះគន់មកលើខ្លួន។ ក្នុងន័យនេះ ភាពខ្វះខាតរបស់វានឹងមិនមានប្រៀបជាងសក្តានុពលដែលអាចធ្វើឱ្យវិស័យឌីជីថលក្លាយជា កន្លែងមានសុវត្ថិភាពជាងមុននោះទេ។

២.៤. ប្រកាសស្តីពីការគ្រប់គ្រងសន្តិសុខសាយប័រ

ប្រកាសស្តីពីការគ្រប់គ្រងសន្តិសុខសាយប័រត្រូវបានចេញដោយក្រសួងប្រៃសណីយ៍ និង ទូរគមនាគមន៍ក្នុងប្រទេសកម្ពុជាក្នុងឆ្នាំ ២០១៨។ ប្រកាសនេះមានគោលបំណងក្នុងការបង្កើត គោលការណ៍ណែនាំ និងស្តង់ដារសម្រាប់ការគ្រប់គ្រងសន្តិសុខ សាយប័រនៅក្នុងប្រទេស និង កំណត់បទប្បញ្ញត្តិមួយចំនួនទាក់ទងនឹងការអនុវត្ត និងនីតិវិធីសន្តិសុខសាយប័រ ដូចជា ការបង្កើត ក្របខណ្ឌការគ្រប់គ្រងសន្តិសុខសាយប័រជាដើមដែលបង្ហាញអំពីតួនាទី និងការទទួល ខុសត្រូវ របស់ភាគីពាក់ព័ន្ធផ្សេងៗ រួមមានស្ថាប័នរដ្ឋាភិបាល អង្គការវិស័យឯកជន និងបុគ្គលទូទៅ។ ប្រកាសនេះតម្រូវឱ្យបណ្តាស្ថាប័នទាំងនោះធ្វើការវាយតម្លៃហានិភ័យសន្តិសុខសាយប័រជាប្រចាំ ដើម្បីកំណត់ពីការគំរាមកំហែង និងភាពងាយរងគ្រោះដែលអាចកើតមានឡើង និងបង្កើតយុទ្ធ សាស្ត្រកាត់បន្ថយហានិភ័យឱ្យបានសមស្រប។ លើសពីនេះ ក៏មានការតម្រូវឱ្យស្ថាប័នទាំងនោះ បង្កើត និងរក្សាផែនការឆ្លើយតបទៅលើ ឧបទ្វីហេតុណាមួយ ដើម្បីធានាថា ពួកគេបានរៀបចំ ដើម្បីឆ្លើយតបប្រកបដោយប្រសិទ្ធភាពចំពោះឧប្បត្តិហេតុសន្តិសុខសាយប័រ។ ស្ថាប័នទាំងនោះក៏ ត្រូវតែផ្តល់ការយល់ដឹង និងកម្មវិធីបណ្តុះបណ្តាលអំពីសន្តិសុខសាយប័រ ជាទៀងទាត់ដល់បុគ្គលិក របស់ពួកគេ ដើម្បីបង្កើនការយល់ដឹងអំពីការគំរាមកំហែងដែលអាចកើតមាន និងធានាថាបុគ្គលិក ត្រូវតែមានជំនាញ និងចំណេះដឹង ដែលចាំបាច់ដើម្បីការពារនិងឆ្លើយតបទៅនឹងឧប្បត្តិហេតុ

សន្តិសុខ សាយបំរើ។ ឧប្បត្តិហេតុសន្តិសុខសាយបំរើដែលពាក់ព័ន្ធនឹងអាជ្ញាធរត្រូវតែរាយការណ៍អំពីគោលការណ៍ណែនាំសម្រាប់ ការរាយការណ៍ និងការចែករំលែកព័ត៌មានក្នុងករណីដែលមានឧបទ្វហេតុសន្តិសុខសាយបំរើ ត្រូវតែបានផ្តល់ឱ្យ។

តាមរយៈការលើកកម្ពស់អំពីវិធីសាស្ត្រផ្នែកលើហានិភ័យចំពោះការគ្រប់គ្រងសន្តិសុខសាយបំរើនិងតម្រូវឱ្យស្ថាប័ននានា

បង្កើតគោលនយោបាយ និងនីតិវិធីដ៏សមស្រប ដែលប្រកាសនេះជួយធានាថាស្ថាប័ន ទាំងនោះបានរៀបចំ កាន់តែប្រសើរឡើងក្នុងការការពារ និងឆ្លើយតបចំពោះឧប្បត្តិហេតុសន្តិសុខសាយបំរើ។ ទោះជាយ៉ាងណាក៏ដោយ ប្រសិទ្ធភាពនៃប្រកាសនេះនឹងអាស្រ័យទៅលើការអនុវត្ត ក៏ដូចជាកម្រិតនៃ ការយល់ដឹងអំពីបញ្ហាសន្តិសុខសាយបំរើក្នុងចំណោមភាគីពាក់ព័ន្ធនានាក្នុងប្រទេស។ ទោះជាយ៉ាងណាក៏ដោយ ប្រកាសនេះនៅតែមានចំណុចខ្វះខាតមួយចំនួន។ ចំណុចទីមួយនោះគឺវិសាលភាពនៅមានកម្រិត។

ប្រកាសនេះផ្តោតជាចម្បងលើការគ្រប់គ្រងសន្តិសុខសាយបំរើក្នុងវិស័យឯកជន និងមិនបានផ្តល់ការណែនាំដ៏ ទូលំទូលាយសម្រាប់ ស្ថាប័នរដ្ឋាភិបាល ឬប្រតិបត្តិករសំខាន់ៗនោះឡើយ។ បើដូចនោះ ប្រសិទ្ធភាពនៃប្រកាសនេះគឺនៅមានកម្រិតក្នុងការដោះស្រាយការគំរាមកំហែងផ្នែក សន្តិសុខសាយបំរើដែលអាចប៉ះពាល់ដល់សន្តិសុខជាតិរបស់ប្រទេស។ ប្រកាសនេះក៏ត្រូវបានគេរិះគន់ផងដែរ ទៅលើកង្វះខាតយន្តការអនុវត្ត។ ប្រកាសនេះមិនបានបញ្ជាក់ពីការពិន័យ ឬការដាក់ទណ្ឌកម្មចំពោះការមិនអនុលោមទៅតាមច្បាប់ ដែលអាចកំណត់ពីប្រសិទ្ធភាពក្នុងការលើកកម្ពស់ឧត្តមនវានុវត្តន៍ អំពី សន្តិសុខសាយបំរើ និងបង្កើតការលើកទឹកចិត្តសម្រាប់ស្ថាប័ននានាក្នុងការកែលម្អឥរិយាបថសន្តិសុខសាយបំរើរបស់ពួកគេ។ ការព្រួយបារម្ភមួយទៀតគឺដោយសារតែភាពមិនច្បាស់លាស់ក្នុងបទប្បញ្ញត្តិមួយចំនួន។ បទប្បញ្ញត្តិមួយចំនួននៅក្នុងប្រកាសមិនត្រូវបានកំណត់ឱ្យបានច្បាស់លាស់នោះទេ ដូចជាតម្រូវការសម្រាប់ផែន ការឆ្លើយតបឧប្បត្តិហេតុ ឬលក្ខណៈវិនិច្ឆ័យសម្រាប់ការវាយតម្លៃហានិភ័យ។ ការណ៍នេះ អាចនាំឱ្យមានការបកស្រាយ និងការអនុវត្តប្រកាសមិនស៊ីសង្វាក់គ្នានៅទូទាំងស្ថាប័នផ្សេងៗ។ ជាចុងក្រោយ ការយល់ដឹងជាសាធារណៈអំពីយន្តការច្បាប់នេះនៅមានកម្រិតទាបនៅឡើយ។ នៅមានភាព ខ្វះខាតលើការយល់ដឹងជាសាធារណៈ និងការយល់ដឹងអំពីបញ្ហាសន្តិសុខសាយបំរើនៅប្រទេសកម្ពុជា ដែលអាចកំណត់ពីប្រសិទ្ធភាពនៃប្រកាសក្នុងការលើកកម្ពស់ឧត្តមនវានុវត្តន៍អំពីសន្តិសុខសាយបំរើនិងការបង្កើតវប្បធម៌នៃការយល់ដឹងអំពីសន្តិសុខសាយបំរើក្នុងចំណោមភាគីពាក់ព័ន្ធនានា។

២.៥. អនុក្រឹត្យស្តីពីការបង្កើតគណៈកម្មាធិការជាតិសន្តិសុខសាយបំរើ

អនុក្រឹត្យស្តីពីការបង្កើតគណៈកម្មាធិការជាតិសន្តិសុខសាយបំរើត្រូវបានចេញដោយរដ្ឋាភិបាលកម្ពុជាក្នុងឆ្នាំ២០២០។ អនុក្រឹត្យនេះមានគោលបំណងបង្កើតយុទ្ធសាស្ត្រ និងក្របខ័ណ្ឌសន្តិសុខសាយបំរើថ្នាក់ជាតិ (Pradeep, 2021) និងបង្កើតស្ថាប័នកណ្តាលមួយដែលទទួលខុសត្រូវ

ក្នុងការសម្របសម្រួល និងត្រួតពិនិត្យកិច្ចខិតខំប្រឹងប្រែង ទៅលើសន្តិសុខសាយបំរែរបស់ស្ថាប័ន រដ្ឋាភិបាល និងអង្គការវិស័យឯកជនផ្សេងៗទៀត។ គណៈកម្មាធិការជាតិសន្តិសុខសាយបំរែមាន សមាសភាពមកពីតំណាងស្ថាប័នរដ្ឋាភិបាល និងស្ថាប័នឯកជននានា រួមមានក្រសួងប្រៃសណីយ៍ និងទូរគមនាគមន៍ អគ្គស្នងការនគរបាលជាតិ ក្រសួងការពារជាតិ និងក្រសួងមហាផ្ទៃ។ អនុក្រឹត្យ នេះបង្កើតគណៈកម្មាធិការជាតិសន្តិសុខសាយបំរែដែលជាស្ថាប័នទទួលខុសត្រូវចម្បង ក្នុងការ សម្របសម្រួល និងត្រួតពិនិត្យកិច្ចខិតខំប្រឹងប្រែងផ្នែកសន្តិសុខសាយបំរែនៅប្រទេសកម្ពុជា។ គណៈកម្មាធិការ ជាតិសន្តិសុខសាយបំរែមានទំនួលខុសត្រូវក្នុងការអភិវឌ្ឍ និងអនុវត្តយុទ្ធសាស្ត្រ និងក្របខ័ណ្ឌសន្តិសុខសាយបំរែជាតិ ក៏ដូចជាការសម្របសម្រួលកិច្ចខិតខំ ប្រឹងប្រែង ផ្នែកសន្តិ សុខសាយបំរែរបស់ ភ្នាក់ងាររដ្ឋាភិបាល និងអង្គការវិស័យឯកជនផ្សេងៗ ទាំងអស់។ អនុក្រឹត្យនេះ តម្រូវឱ្យគណៈកម្មាធិការជាតិសន្តិសុខសាយបំរែផ្តល់របាយការណ៍ជាប្រចាំអំពីបញ្ហាសន្តិ សុខសាយបំរែជូននាយករដ្ឋមន្ត្រី ហើយស្ថាប័នរដ្ឋាភិបាល និងបណ្តាស្ថាប័នវិស័យឯកជននានា រាយការណ៍អំពីឧប្បត្តិហេតុសន្តិសុខសាយបំរែទៅគណៈកម្មាធិការជាតិសន្តិសុខសាយបំរែ។

លើសពីនេះ រដ្ឋាភិបាលកម្ពុជាក៏បានបង្កើតក្រុមការងារប្រព័ន្ធផ្សព្វផ្សាយសង្គមថ្មីក្នុងឆ្នាំ ២០១៤ ដើម្បីតាមដានសកម្មភាពអនឡាញនៅក្នុងវេទិកាឌីជីថលដូចជាគេហទំព័រ Facebook Twitter Google-plus Blogs YouTube និងប្រព័ន្ធផ្សព្វផ្សាយផ្សេងទៀត។ និយាយជាផ្លូវការគឺថា ពិតជាមានភាពចាំបាច់ក្នុងការការពារជំហរ និងកិត្យានុភាពរបស់រដ្ឋាភិបាល (Blomberg, 2014)។

សរុបមក អនុក្រឹត្យស្តីពីការបង្កើតគណៈកម្មាធិការជាតិសន្តិសុខសាយបំរែបង្ហាញពីជំហានឆ្ពោះ ទៅមុខយ៉ាងសំខាន់ក្នុងការបង្កើតស្ថាប័នមជ្ឈឹមដែលទទួលខុសត្រូវក្នុងការសម្របសម្រួល និង ត្រួតពិនិត្យកិច្ចខិតខំប្រឹងប្រែងផ្នែកសន្តិសុខសាយបំរែ នៅប្រទេសកម្ពុជា។ តាមរយៈការបង្កើតយុទ្ធ សាស្ត្រ និងក្របខ័ណ្ឌសន្តិសុខសាយបំរែថ្នាក់ជាតិ និងការលើកកម្ពស់ ការសម្របសម្រួល និងការ ចែករំលែកព័ត៌មានក្នុងចំណោមភាគីពាក់ព័ន្ធផ្សេងៗ។ អនុក្រឹត្យនេះជួយធានាថា ប្រទេសកម្ពុជា បានរៀបចំកាន់តែ ប្រសើរឡើងដើម្បីការពារ និងឆ្លើយតបទៅនឹងការគំរាមកំហែងផ្នែកសន្តិ សុខសាយបំរែ។ ទោះជាយ៉ាងណាក៏ដោយ ប្រសិទ្ធភាពនៃអនុក្រឹត្យនេះនឹងអាស្រ័យទៅលើការ អនុវត្ត និងការពង្រឹងក៏ដូចជាកម្រិតនៃការប្តេជ្ញាចិត្ត និងសហប្រតិបត្តិការរវាងភាគីពាក់ព័ន្ធផ្សេងៗ ក្នុងប្រទេស។

អនុក្រឹត្យនេះផ្តោតសំខាន់លើស្ថាប័នរដ្ឋាភិបាលដោយការចូលរួមពីសំណាក់វិស័យឯកជននៅមាន កម្រិត។ ដោយសារវិស័យឯកជនគឺជាគោលដៅសំខាន់សម្រាប់ការវាយប្រហារតាមអ៊ីនធឺណិត ពិតជាមានសារៈសំខាន់ណាស់ក្នុងការធានាថា វិស័យឯកជនបានចូលរួមយ៉ាង សកម្មក្នុងកិច្ច ខិតខំប្រឹងប្រែងទៅលើសន្តិសុខសាយបំរែ។ ហើយក៏នៅមានការខ្វះខាតផងដែរអំពីព័ត៌មានលម្អិត អំពីយុទ្ធសាស្ត្រសន្តិសុខសាយបំរែថ្នាក់ជាតិ។ ខណៈពេលដែលអនុក្រឹត្យនេះអំពាវនាវឱ្យមានការ បង្កើតយុទ្ធសាស្ត្រសន្តិសុខសាយបំរែជាតិ អនុក្រឹត្យនេះមិនបាន លម្អិតអំពីព័ត៌មានជាក់លាក់នៃ យុទ្ធសាស្ត្រនោះទេ។ នេះអាចនាំឱ្យមានភាពមិនស៊ីសង្វាក់គ្នាក្នុងការបកស្រាយ និងការអនុវត្ត យុទ្ធសាស្ត្រទៅលើភាគីពាក់ព័ន្ធផ្សេងៗទាំងអស់។ អនុក្រឹត្យនេះរៀបរាប់អំពីមុខងារ

និងសមាសភាពនៃគណៈកម្មាធិការជាតិសន្តិសុខសាយប័រ ប៉ុន្តែអាចមានភាពមិនច្បាស់លាស់នៃ តួនាទី និងការទទួល ខុសត្រូវរបស់សមាជិកម្នាក់ៗ និងស្ថាប័ននានាដែលចូលរួម។ ការរិះគន់ក៏ បានផ្ដោតលើយន្តការ អនុវត្តដែលមានកម្រិតរបស់អនុក្រឹត្យនេះផងដែរ ដោយសារតែការពិន័យ ការដាក់ទណ្ឌកម្មចំពោះការមិនបាន អនុលោមទៅតាមច្បាប់ មិនត្រូវបានបញ្ជាក់ដែលអាចធ្វើឱ្យ មិនសូវមានប្រសិទ្ធភាពក្នុងការលើកកម្ពស់ ឧត្តមនវានុវត្តន៍ទៅលើសន្តិសុខសាយប័រនិងបង្កើត ការលើកទឹកចិត្តសម្រាប់ស្ថាប័ននានាក្នុងការកែលម្អឥរិយាបថទៅលើសន្តិសុខសាយប័ររបស់ ពួកគេ។

៣. កិច្ចពិភាក្សា៖ ជំហានបន្ទាប់ ?

ផ្នែកទាំងពីរខាងលើ បានបង្ហាញពីរបៀបដែលប្រជាប្រិយភាពនៃអ៊ិនធឺណិតបាននាំមកនូវការ អភិវឌ្ឍសង្គម សេដ្ឋកិច្ច និងនយោបាយគួរឱ្យកត់សម្គាល់នៅក្នុងប្រទេសកម្ពុជា។ ដោយមើល ឃើញពីសារៈសំខាន់នៃការផ្លាស់ប្តូរទាំងនេះនៅក្នុង វិស័យឌីជីថលដែលជាគំនិតថ្មី ដូច នេះបទប្បញ្ញត្តិច្បាប់ថ្មីនេះបានក្លាយជារឿងចាំបាច់ដើម្បីគ្រប់គ្រងការប្រើប្រាស់អ៊ិនធឺណិត។ ការ វាយតម្លៃអំពីស្ថានភាពនៃច្បាប់ឧក្រិដ្ឋកម្មតាមអ៊ិនធឺណិតបានបង្កើតលទ្ធផលសំខាន់ៗ។ ទីមួយ ប្រទេសកម្ពុជាបានចាត់ វិធានការសំខាន់ៗ ដើម្បីកែលម្អទិដ្ឋភាពសន្តិសុខសាយប័ររបស់ខ្លួន។ នេះ គឺជារឿងដែលគួរឱ្យកត់សម្គាល់ និងជាការអភិវឌ្ឍ ចាំបាច់បំផុត ដោយសារកង្វះបទប្បញ្ញត្តិផ្លូវ ច្បាប់សម្រាប់អ៊ិនធឺណិតហើយក៏ជារឿងសំខាន់ដោយសារការកើនឡើងនៃករណី គំរាមកំហែង ទាក់ទងនឹងការប្រើប្រាស់អ៊ិនធឺណិត ដែលមិនត្រឹមតែប៉ះពាល់ដល់ប្រទេសកម្ពុជាប៉ុណ្ណោះទេ ប៉ុន្តែ នៅក្នុងតំបន់ ទាំងមូល។ ទោះបីជាបទប្បញ្ញត្តិផ្លូវច្បាប់មួយចំនួនមាននៅក្នុងក្រមព្រហ្មទណ្ឌដោះ ស្រាយបទល្មើសទាក់ទងនឹងកុំព្យូទ័រក៏ដោយ ក៏កំណែទម្រង់ច្បាប់គឺជារឿងចាំបាច់ដែរ។ លទ្ធផល ទីពីរនៃទិដ្ឋភាពទូទៅនៃការអភិវឌ្ឍផ្នែកច្បាប់សំខាន់ៗមួយចំនួនដែលគ្រប់គ្រងឧក្រិដ្ឋកម្ម តាមអ៊ិនធឺណិតគឺថា ទោះបីជាច្បាប់ថ្មីត្រូវបានបង្កើត ឬកំពុងត្រូវបានព្រាងក៏ដោយក៏វានៅតែ បង្ហាញពីបញ្ហាប្រឈមបន្ទាន់ដែលត្រូវដោះស្រាយ។ អត្ថបទដែលនៅសល់ក្នុងផ្នែកទី៣ នេះនឹង រៀបរាប់អំពីដំណោះស្រាយមួយចំនួន។

ទី១ គឺការយល់ដឹងជាសាធារណៈ។ បញ្ហាប្រឈមចម្បងមួយ គឺកង្វះការយល់ដឹងអំពីសុវត្ថិភាព អ៊ិនធឺណិត (Corrado and Sakal, 2021) ក្នុងចំណោមស្ថាប័នសាធារណៈ និងឯកជនទូទៅ។ បុគ្គល និងអង្គការជាច្រើននៅក្នុងប្រទេសកម្ពុជាមិនបានដឹងពីហានិភ័យនៃការគំរាមកំហែង តាមអ៊ិនធឺណិត និងមិនបានចាត់វិធានការប្រុងប្រយ័ត្នជាចាំបាច់ដើម្បីការពារទ្រព្យសម្បត្តិឌីជីថល របស់ពួកគេ។ ករណីនេះធ្វើឱ្យពួកគេងាយរងគ្រោះទៅនឹងការវាយប្រហារតាមអ៊ិនធឺណិត ដូចជា ការបោកបញ្ឆោត ឬការឆ្លងមេរោគ។ ដូចនេះ ការអប់រំ ជាពិសេសអក្ខរកម្មឌីជីថលគឺជាយុទ្ធសាស្ត្រ គន្លឹះដើម្បីបង្កើនការយល់ដឹងរបស់មនុស្សអំពីបញ្ហាសុវត្ថិភាពអ៊ិនធឺណិត និងធ្វើឱ្យពួកគេដឹងពីវិធី ការពារខ្លួនពីការវាយប្រហារតាមអ៊ិនធឺណិត ឬវិធីកាត់បន្ថយហានិភ័យនៃការក្លាយជាជនរងគ្រោះ។

ទី២ ធនធានមានកំណត់។ បញ្ហាប្រឈមមួយទៀត គឺធនធាននៅមានកម្រិតសម្រាប់គំនិតដួចផ្តើម ផ្នែកសុវត្ថិភាពអ៊ិនធឺណិតនៅកម្ពុជា (ASEAN, 2022)។ បញ្ហាប្រឈមរួមបញ្ចូលទាំងកង្វះ មូលនិធិ ក៏ដូចជាកង្វះអ្នកជំនាញផ្នែកសន្តិសុខសាយប័រ ដែលធ្លាប់បានទទួលបានការបណ្តុះ

បណ្តាល។ ប្រសិនបើមិនមានមូលនិធិ និងធនធានសមស្រប វាអាចជាការលំបាកសម្រាប់ រដ្ឋាភិបាល អង្គការ និងវិស័យឯកជន ក្នុងការអនុវត្តវិធានការសន្តិសុខសាយបំរែឱ្យបាន ទូលំ ទូលាយ និងឆ្លើយតបប្រកបដោយប្រសិទ្ធភាពចំពោះឧប្បត្តិហេតុតាមអ៊ិនធឺណិត។ លើសពីនេះ ការវិវឌ្ឍន៍ដ៏លឿននៃបច្ចេកវិទ្យាបង្កបញ្ហាប្រឈមចំពោះសន្តិសុខសាយបំរែនៅកម្ពុជា។ នៅពេល ដែលបច្ចេកវិទ្យាថ្មីលេចឡើង ហានិភ័យនិងការគំរាមកំហែងថ្មីៗក៏កើតឡើងដែរ ហើយស្ថាប័ននានា អាចមានភាពលំបាកក្នុងការអនុវត្តទៅតាមឧត្តមនវានុវត្តន៍សុវត្ថិភាពអ៊ិនធឺណិតចុងក្រោយបំផុត។

ទី៣ កិច្ចសហប្រតិបត្តិការអន្តរជាតិនៅមានកម្រិត។ លើសពីនេះ កង្វះកិច្ចសហប្រតិបត្តិការ (JICA, 2022) និងការសម្របសម្រួលពីអន្តរជាតិក៏អាចបង្កបញ្ហាប្រឈមសម្រាប់សន្តិ សុខសាយបំរែនៅកម្ពុជាផងដែរ។ ដោយសារការគំរាមកំហែងតាមអ៊ិនធឺណិតជាញឹកញាប់ឆ្លងកាត់ ព្រំដែន ប្រទេសនានាត្រូវធ្វើការរួមគ្នាដើម្បីចែករំលែកព័ត៌មាន និងសហការលើគំនិតផ្តួចផ្តើមសន្តិ សុខសាយបំរែ។ លើសពីនេះទៅទៀត កិច្ចខិតខំប្រឹងប្រែងរួមគ្នាក្នុងការអភិវឌ្ឍ និងការប្រកាន់ខ្ជាប់ នូវក្របខ័ណ្ឌអន្តរជាតិដូចជា ក្រុមប្រឹក្សានៃអនុសញ្ញាអឺរ៉ុបស្តីពីឧក្រិដ្ឋកម្មតាមអ៊ិនធឺណិតជាដើម (COE, n.d) គឺជាយុទ្ធសាស្ត្រដ៏សំខាន់ដែលគ្រប់ប្រទេសទាំងអស់ មិនត្រឹមតែកម្ពុជាប៉ុណ្ណោះទេ ដែលអាចកែលម្អបាន។

ទី៤ កិច្ចសហប្រតិបត្តិការក្នុងប្រទេស។ ដូចគ្នាទៅនឹងចំណុចខាងលើ កិច្ចសហប្រតិបត្តិការក្នុង ប្រទេសក៏នៅមានកម្រិតដូចគ្នា (ODC, 2021)។ កិច្ចសហប្រតិបត្តិការអន្តរជាតិមានសារៈសំខាន់ ព្រោះវាជួយតម្រិះទស្សនៈរបស់សហគមន៍អន្តរជាតិស្តីពីសន្តិសុខសាយបំរែ។ លើសពីនេះទៀត វា បន្ថែមគណនេយ្យភាពព្រោះការចុះហត្ថលេខាលើសន្ធិសញ្ញាអន្តរជាតិបង្កើតប្រព័ន្ធត្រួតពិនិត្យ និង តុល្យភាពដែលតាមទ្រឹស្តីគួរតែការពារអ្នកប្រើប្រាស់អ៊ិនធឺណិត។ ទោះជាយ៉ាងណាក៏ដោយ កិច្ចសហប្រតិបត្តិការ ក្នុងប្រទេសរវាងភាគីពាក់ព័ន្ធសំខាន់ៗ គឺចាំបាច់ដើម្បីឱ្យមានកិច្ចសហ ប្រតិបត្តិការអន្តរជាតិ។ កិច្ចសហប្រតិបត្តិការត្រូវតែកើតឡើងរវាងរដ្ឋាភិបាល និងភ្នាក់ងារសំខាន់ៗ ដូចជា អង្គការសង្គមស៊ីវិល (CSOs) សកម្មជន វិស័យប្រព័ន្ធផ្សព្វផ្សាយ វិស័យអប់រំ និងអ្នក នយោបាយ ឬក្រុមផ្សេងទៀតដែលតំណាងឱ្យផលប្រយោជន៍នៃក្រុមសង្គមណាមួយ។ កិច្ចសហ ប្រតិបត្តិការបែបនេះមានសារៈសំខាន់ដើម្បីឱ្យការបង្កើតក្របខ័ណ្ឌ ច្បាប់ទាក់ទងនឹងវិស័យឌីជីថល ត្រូវបានធ្វើឡើងប្រកបដោយការឯកភាពពីអង្គភាពទាំងអស់ ដែលលទ្ធផលនីមួយៗអាចត្រូវបាន ចរចា និងយល់ស្របដោយទាំងអស់គ្នា។

២. សេចក្តីសន្និដ្ឋាន

ក្នុងទស្សន៍វិស័យចុងក្រោយនេះ កម្ពុជាសម្រេចបាននូវវឌ្ឍនភាពគួរឱ្យកត់សម្គាល់ក្នុងការអភិវឌ្ឍច្បាប់ សន្តិសុខសាយបំរែ ដើម្បីធ្វើឱ្យវិស័យឌីជីថលកាន់តែមានសុវត្ថិភាព។ ការអភិវឌ្ឍក្របខ័ណ្ឌច្បាប់នៅ ក្នុងវិស័យនេះគឺនៅ តែជារឿងចាំបាច់ដោយសារតែការកើនឡើងនៃភាពពេញនិយមយ៉ាងឆាប់ រហ័សនៃឧបករណ៍ឌីជីថល និងប្រព័ន្ធផ្សព្វផ្សាយ នៅក្នុងប្រទេស។ ខណៈពេលដែលអ៊ិនធឺណិត បាននាំមកនូវឱកាសជាច្រើន រួមទាំងលទ្ធភាពក្នុងការធ្វើឱ្យប្រសើរឡើង នូវការប្រាស្រ័យទាក់ទង គ្នារវាងមនុស្ស និងតួអង្គសង្គមស៊ីវិលផ្សេងទៀត ឬការទទួលបានព័ត៌មានផ្សេងៗ និងចម្រុះកាន់តែ

ច្រើន ការអភិវឌ្ឍយ៉ាងឆាប់រហ័សនៃវិស័យឌីជីថលនេះក៏បានបង្ហាញពីបញ្ហាប្រឈមជាច្រើន ផងដែរ ដូចជា ឧក្រិដ្ឋកម្មតាមអ៊ីនធឺណិត ឬការកំណត់ថាតើនរណា និងរបៀបគ្រប់គ្រងបែបណា ដែលគួរគ្រប់គ្រងទៅលើសកម្មភាពនានាដែលកើតឡើងនៅក្នុងពិភពនិម្មិតនេះ។

ការពិនិត្យមើលពីដំណើរការនៃច្បាប់សំខាន់ៗចំនួនប្រាំនេះ រួមមានច្បាប់ស្តីពីការគ្រប់គ្រងវិស័យ ទូរគមនាគមន៍របស់ប្រទេសជាតិ ច្បាប់ស្តីពីឧក្រិដ្ឋកម្មតាមអ៊ីនធឺណិត អនុក្រឹត្យស្តីពីការបង្កើត អាជ្ញាធរជាតិប្រយុទ្ធនឹងឧក្រិដ្ឋកម្មតាមអ៊ីនធឺណិត ប្រកាសស្តីពីការគ្រប់គ្រងសន្តិសុខសាយបំរែ និង អនុក្រឹត្យស្តីពីការបង្កើតគណៈកម្មាធិការជាតិសន្តិសុខសាយបំរែ បង្ហាញពី លក្ខណៈសំខាន់ៗនៃ ស្ថានភាពបច្ចុប្បន្ននៃច្បាប់សន្តិសុខអ៊ីនធឺណិតនៅកម្ពុជា។ ចំនុចទីមួយ ដូចដែលបានលើកឡើង ពីមុនមក រដ្ឋាភិបាលកម្ពុជាបានកំណត់បញ្ហាប្រឈមមួយចំនួនដែលកំពុងបន្តនៅក្នុង វិស័យឌីជីថល និងបានបង្កើតផែនការកែលម្អសន្តិសុខ នៅក្នុងវិស័យឌីជីថល។ ចំនុចទីពីរ ការ សម្រេចនូវក្របខ័ណ្ឌច្បាប់ដែលដោះស្រាយបញ្ហាប្រឈមជាបន្តបន្ទាប់ដែលបណ្តាលមក ពីភាព ពេញនិយមនៃអ៊ីនធឺណិតទំនងជាមិនអាចកើតឡើងក្នុងប៉ុន្មានឆ្នាំខាងមុខនេះទេ។ ម៉្យាងវិញទៀត ដោយសារតែ វិស័យឌីជីថលស្ថិតក្នុងការវិវឌ្ឍន៍ឥតឈប់ឈរ ហើយរាល់ការអភិវឌ្ឍថ្មីៗនៅក្នុង វិស័យបច្ចេកវិទ្យា បញ្ហាប្រឈមថ្មីៗនឹង លេចឡើង។ ម៉្យាងវិញទៀត ការសម្រេចបាននូវសន្តិ សុខសាយបំរែដ៏រឹងមាំមួយ គឺត្រូវការការធ្វើការផ្ទាល់បន្ថែមទៀតពីភាគីពាក់ព័ន្ធដូចជាសង្គមស៊ីវិល រួមទាំងអង្គការមិនមែនរដ្ឋាភិបាល សកម្មជន វិស័យប្រព័ន្ធផ្សព្វផ្សាយ វិស័យអប់រំ និងវិស័យ ឯកជនទាំងអស់នៅក្នុងប្រទេសកម្ពុជា។ ការធ្វើឱ្យភាគីពាក់ព័ន្ធទាំងអស់ចូលរួមយ៉ាងសកម្មក្នុងការ សន្ទនា ជាមួយរដ្ឋាភិបាលដើម្បីបង្កើតបទដ្ឋានដែលគ្រប់គ្រងលើវិស័យឌីជីថលនៅក្នុង ប្រទេសកម្ពុជានេះ មិនត្រឹមតែមាន សារៈសំខាន់ ក្នុងការធ្វើឱ្យបទប្បញ្ញត្តិទាំងនោះកាន់តែមាន បរិយាប័ន្នតែប៉ុណ្ណោះទេ ថែមទាំងធ្វើឱ្យមាននិរន្តរភាពក្នុងប្រទេស និងក្នុងតំបន់ផងដែរ។

គន្ថទ្រឹស

មាត្រាទី១៩ សេចក្តីព្រាងច្បាប់ស្តីពីឧក្រិដ្ឋកម្មអ៊ីនធឺណិតជាភាសាអង់គ្លេស. ច្បាប់ឧក្រិដ្ឋកម្មតាមអ៊ីនធឺណិត. មាត្រាទី១៩. មាននៅ៖ https://www.article19.org/wp-content/uploads/2018/02/Draft-Law-On-CyberCrime_Englishv1.pdf

អាស៊ាន (ឆ្នាំ២០២២) យុទ្ធសាស្ត្រសហប្រតិបត្តិការសន្តិសុខសាយបំរែអាស៊ាន, យុទ្ធសាស្ត្រសហប្រតិបត្តិការសន្តិសុខសាយបំរែអាស៊ាន. អាស៊ាន. មាននៅ៖ https://asean.org/wp-content/uploads/2022/02/01-ASEAN-Cybersecurity-Cooperation-Paper-2021-2025_final-23-0122.pdf

Blomberg, M. (ឆ្នាំ២០១៤) 'ក្រុមការងារប្រព័ន្ធផ្សព្វផ្សាយសង្គមថ្មីនឹងត្រួតពិនិត្យវេបសាយ', 'ក្រុមការងារប្រព័ន្ធផ្សព្វផ្សាយសង្គមថ្មីនឹងត្រួតពិនិត្យវេបសាយ'. ឌី ខេមបូឌា ដេលី. មាននៅ៖ <https://english.cambodiadaily.com/news/cyber-war-team-to-monitor-web-72677/>

បណ្ឌិត្យសភាបច្ចេកវិទ្យាឌីជីថលកម្ពុជា (CADT) (ឆ្នាំ២០២២) តម្រូវការ និងការផ្គត់ផ្គង់ជំនាញឌីជីថលនៅកម្ពុជា, CADT. មាននៅ៖ <https://www.cadt.edu.kh/resources/digital-skills-assessment-event-2021/demand-for-and-supply-of-digital-skills-in-cambodia-2021/>

COE អនុសញ្ញាទីក្រុង Budapest - ឧក្រិដ្ឋកម្មតាមអ៊ីនធឺណិត. COE. មាននៅ៖ https://www.coe.int/en/web/cybercrime/the-budapest-convention?_82_struts_action=%2Flanguage%2Fview&_82_languageId=fr_FR

Corrado, R. និង សាកល, ម (ឆ្នាំ២០២១) សន្តិសុខសាយបំរែនៅកម្ពុជា៖ ការយល់ដឹងជាជំហានដំបូង, មជ្ឈមណ្ឌលអភិវឌ្ឍន៍កម្ពុជា. មាននៅ៖ https://cd-center.org/wp-content/uploads/2021/08/P124_20210805_V3IS11_EN.pdf
ក្រមព្រហ្មទណ្ឌ (ឆ្នាំ២០០៩) ក្រមព្រហ្មទណ្ឌ. ព្រះរាជាណាចក្រកម្ពុជា. មាននៅ៖ <http://www.skpcambodia.com/PDF/storage/uploads/files/Criminal%20and%20Criminal%20Procedure%20Laws/criminal-code%20Eng.pdf> (បានចូលមើលនៅថ្ងៃទី១៨ ខែមីនា ឆ្នាំ២០២៣)។

Flynn, G. (ឆ្នាំ២០១៩) បញ្ហាប្រឈមផ្នែកសន្តិសុខសាយបំរែរបស់កម្ពុជា, CapitalCambodia. មាននៅ៖ <https://capitalcambodia.com/cambodias-cybersecurity-challenges/>

HRW (ឆ្នាំ២០២១) កម្ពុជា៖ សេចក្តីព្រាងច្បាប់ស្តីពីឧក្រិដ្ឋកម្មតាមអ៊ីនធឺណិត, អង្គការឃ្លាំមើលសិទ្ធិមនុស្ស. មាននៅ៖ <https://www.hrw.org/news/2020/11/13/cambodia-scrap-draft-cybercrime-law>

IPI (ឆ្នាំ២០២០) ច្បាប់ឧក្រិដ្ឋកម្មតាមអ៊ីនធឺណិតនៅកម្ពុជានឹងរារាំងសេរីភាពសារព័ត៌មាន, វិទ្យាស្ថានសារព័ត៌មានអន្តរជាតិ. មាននៅ៖ <https://ipi.media/cambodia-cybercrime-law-will-stifle-press-freedom/>

ទីភ្នាក់ងារសហប្រតិបត្តិការអន្តរជាតិជប៉ុន (JICA) (ឆ្នាំ២០២២) ការចុះហត្ថលេខាលើកំណត់ហេតុនៃកិច្ចពិភាក្សាលើគម្រោងសហប្រតិបត្តិការបច្ចេកទេសជាមួយប្រទេសកម្ពុជា៖ គម្រោងកែលម្អភាពធន់នឹងអ៊ីនធឺណិត. JICA. មាននៅ៖ https://www.jica.go.jp/english/news/press/2022/20221205_41.html

Kelliher, F. (ឆ្នាំ២០២៣) សំណើច្បាប់ដែលលេចធ្លាយនឹងផ្តល់អំណាចបន្ថែមដល់កម្ពុជាក្នុងការចាប់ពីរដ្ឋអ្នករិះគន់, Rest of World. មាននៅ៖ <https://restofworld.org/2023/cybersecurity-law-draft-cambodia-elections/>

Kemp, S. (ឆ្នាំ២០២៣) ឌីជីថលឆ្នាំ២០២៣៖ កម្ពុជា - DataReportal - Global Digital Insights, DataReportal. DataReportal - Global Digital Insights. មាននៅ៖ <https://datareportal.com/reports/digital-2023-cambodia>

Levi, M. និង Stoker, L. (ឆ្នាំ២០០០) "ទំនុកចិត្តនយោបាយ និងភាពជឿជាក់", Annual Review of Political Science, ៣(១), ទំព័រទី ៤៧៥-៥០៧. មាននៅ៖ <https://doi.org/10.1146/annurev.polisci.3.1.475>.

MPTC (ឆ្នាំ២០២២) គោលនយោបាយរដ្ឋាភិបាលឌីជីថលកម្ពុជា ២០២២-២០៣៥, ក្រសួងប្រៃសណីយ៍ និងទូរគមនាគមន៍. មាននៅ៖ <https://mptc.gov.kh/en/documents/policies/28365/>

ណារិន, ស (ឆ្នាំ២០២០) សកម្មជន៖ សេចក្តីព្រាងច្បាប់ស្តីពីឧក្រិដ្ឋកម្មតាមអ៊ីនធឺណិតរបស់កម្ពុជា ធ្វើឱ្យប៉ះពាល់ដល់ការបញ្ចេញមតិនិងឯកជនភាព. វិអូអេ. វិទ្យុសំឡេងសហរដ្ឋអាមេរិក (VOA News). មាននៅ៖ https://www.voanews.com/a/east-asia-pacific_activists-cambodias-draft-cybercrime-law-imperils-free-expression-privacy/6196959.html

អូឌីស៊ី អង្គការទិន្នន័យអំពីការអភិវឌ្ឍ, អង្គការទិន្នន័យអំពីការអភិវឌ្ឍ (អូឌីស៊ី). មាននៅ៖ <https://opendevelopmentcambodia.net/tag/digital-economy/>

អូឌីស៊ីប អង្គការទិន្នន័យអំពីការអភិវឌ្ឍ, អង្គការទិន្នន័យអំពីការអភិវឌ្ឍ (អូឌីស៊ី). មាននៅ៖
<https://opendevdevelopmentcambodia.net/tag/draft-cybercrime-law/#!/story=post-127300>

អូឌីស៊ី (ឆ្នាំ២០២១) កម្ពុជាត្រៀមខ្លួនរួចជាស្រេច ដើម្បីចូលរួមជាមួយបណ្តាប្រទេសសមាជិកអាស៊ាន ដើម្បីឆ្ពោះទៅកាន់លំហសាយបំរើ មួយដែលមានសុវត្ថិភាព និងប្រកបដោយបរិយាប័ន្ន. អង្គការទិន្នន័យអំពីការអភិវឌ្ឍកម្ពុជា. មាននៅ៖
<https://opendevdevelopmentcambodia.net/news/cambodia-pledges-cooperation-in-push-for-inclusive-cyberspace/#!/story=post-155739>

Phong, K., Srou, L. និង Solá, J. (ឆ្នាំ ២០១៦) ទូរស័ព្ទដៃ និងការប្រើប្រាស់អ៊ីនធឺណិតកម្ពុជា ២០១៦ - មូលនិធិអាស៊ី, មូលនិធិអាស៊ី. មាននៅ៖
https://asiafoundation.org/wp-content/uploads/2016/12/Mobile-Phones-and-Internet-Use-in-Cambodia-2016.pdf?source=post_page----

Pradeep, A. (ឆ្នាំ២០២២) កម្ពុជាពង្រឹងវិធានការការពារទិន្នន័យផ្ទាល់ខ្លួន - ខ្មែរថាមស៍, ខ្មែរថាមស៍ - ការយល់ដឹងអំពីប្រទេសកម្ពុជា. មាននៅ៖
<https://www.asiapropertyawards.com/en/cambodia-improves-digital-infrastructure-with-digital-roadmap-2021-2035/>

Property Report (ឆ្នាំ២០២២) កម្ពុជាកែលម្អហេដ្ឋារចនាសម្ព័ន្ធខ្លីជីវិតជាមួយនឹងផែនទីបង្ហាញផ្លូវខ្លីជីវិត ២០២១-២០៣៥, Asia Property Awards. មាននៅ៖
<https://www.asiapropertyawards.com/en/cambodia-improves-digital-infrastructure-with-digital-roadmap-2021-2035/>

សេង, ម. (ឆ្នាំ២០២២) ការព្រួយបារម្ភបានលើកឡើងជុំវិញសេចក្តីព្រាងច្បាប់ស្តីពីឧក្រិដ្ឋកម្មតាមអ៊ីនធឺណិត. គីរីប៉ូស្ត. មាននៅ៖ <https://kiripost.com/stories/fears-raised-over-cybercrime-draft-law>

Tunggal, T. (ឆ្នាំ២០២៣) ហេតុអ្វីសន្តិសុខតាមអ៊ីនធឺណិតមានសារៈសំខាន់?, RSS.មាននៅ៖
<https://www.upguard.com/blog/cybersecurity-important>

UNESCO (ឆ្នាំ២០២០) កម្ពុជា៖ ការអប់រំតាមប្រព័ន្ធខ្លីជីវិត គឺនឹងនៅទីនេះ, IIEP. មាននៅ៖
<https://www.iiep.unesco.org/en/cambodia-digital-education-here-stay-13492>

Vong, M. and Hok, K. (ឆ្នាំ២០១៨) "Facebooking," South East Asia Research, ២៦(៣) ទំព័រ ២១៩-២៣៤. មាននៅ៖ <https://doi.org/10.1177/0967828x17754113>.

WTO (ឆ្នាំ២០១៥) WTACCKHM5 leg 10 - អង្គការពាណិជ្ជកម្មពិភពលោក, WTO.
មាននៅ៖

https://www.wto.org/english/thewto_e/acc_e/khm_e/WTACCKHM5_LEG_10.pdf

✉ contact@opendevcam.net

☎ +៨៥៥ ២៣ ៩០២ ១៩៦

f Open Development Cambodia

in Open Development Cambodia Organization

X Open Development Cambodia Organization

▶ Open Development Cambodia Organization

🌐 www.opendevdevelopmentcambodia.net

🏠 ផ្ទះលេខ ២៣២ ផ្លូវលេខ ៦០៦ សង្កាត់បឹងកក់ទី២ ខណ្ឌទួលគោក រាជធានីភ្នំពេញ ព្រះរាជាណាចក្រកម្ពុជា

