မြန်မာနိုင်ငံ၏ အိုင်စီတီဂေဟစနစ် လေ့လာမှု - အနှစ်ချုပ်

၂၀၂၂ ခုနှစ်၊ ဇူလိုင်လ (၁၅) ရက်နေ့တွင် တယ်လီနောနှင့် အရပ်ဘက်အဖွဲ့အစည်း ၄၇၄ ဖွဲ့ ကိုယ်စား Centre for Research on Multinational Corporations (SOMO) တို့အကြား သဘောတူခဲ့သည့် နားလည်မှုစာချွန်လွှာ (MOU) တွင်ပါဝင်သူများမှ လုပ်ငန်းအပ်နှံထားသော အများပြည်သူ ရရှိနိုင်သည့် လျှို့ဝှက်လေ့လာမှုတစ်ခု၏ အနှစ်ချုပ်

threefold

၂၀၂၄ ခုနှစ်၊ ဖေဖော်ဝါရီလ

မာတိကာ

မြန်မာနိုင်ငံ အိုင်စီတီဂေဟစနစ် လေ့လာမှုနှင့် ဤအနှစ်ချုပ်အစီရင်ခံစာကို တယ်လီနောနှင့် အရပ်ဘက်အဖွဲ့အစည်းပေါင်း ၄၇၄ ဖွဲ့ကိုယ်စား Centre for Research on Multinational Corporations (SOMO) တို့အကြား ၂၀၂၂ ခုနှစ်၊ ဇူလိုင်လ ၁၅ ရက်နေ့တွင် သဘောတူခဲ့သည့် နားလည်မှုစာချွန်လွှာ (MOU) ပါဝင်သူများ၏ လုပ်ငန်းအပ်နှံမှုအရ Threefold Sustainability မှ ပြင်ဆင်ထားပါသည်။ Threefold Sustainability သည် စီးပွားရေးနှင့် လူ့အခွင့်အရေးနှင့် အိုင်စီတီကဏ္ဍဆိုင်ရာ ကျွမ်းကျင်မှုများဖြင့် ရေရှည်တည်တံ့ခိုင်မြဲမှုအတွက် အတိုင်ပင်ခံလုပ်ငန်းတစ်ရပ်ဖြစ်ပါသည်။

ဤအစီရင်ခံစာ၏ နိဂုံးချုပ်အချက်များသည် Threefold Sustainability ၏ လုပ်ငန်းပိုင်းဆိုင်ရာ ကျွမ်းကျင်မှုဖြင့် စီရင်ဆုံးဖြတ်ခြင်းကို ကိုယ်စားပြုပြီး ဤအစီရင်ခံစာပါ အချက်အလက်များ တိကျသေချာစေရန်အတွက် ရည်ရွယ်ချက်ကောင်းများဖြင့် ကြိုးပမ်းအားထုတ်မှုများ ပြုလုပ်ခဲ့သော်လည်း၊ အစီရင်ခံစာသည် အခြားသော ကြားခံအဖွဲ့အစည်းများမှ ပေးဆောင်သော အချက်အလက်များအပေါ် မှီခိုအားထားနေပြီး ၎င်း၏ပြည့်စုံမှု သို့မဟုတ် မှန်ကန်မှုကို အာမခံနိုင်မည်မဟုတ်ပေ။ ဤအစီရင်ခံစာပါ အချက်အလက်များကို အသုံးပြုခြင်း သို့မဟုတ် မှီခိုအားထားခြင်းကြောင့် ဖြစ်ပေါ်လာသော မည်သည့်အမှားအယွင်းများ၊ ချန်လှပ်မှုများ သို့မဟုတ် အကျိုးဆက်များအတွက် စာရေးသူတို့မှ တာဝန်မရှိပါ။

၁။ နိဒါန်း

၂၀၂၁ ခုနှစ်၊ နွေလိုင်လတွင် အရပ်ဘက်အဖွဲ့အစည်းပေါင်း ၄၇၄ ဖွဲ့မှ OECD ၏ Norwegian National Contact Point ဖြင့် တယ်လီနော - Telenor ASA အား တိုင်ကြားခဲ့ရာ တယ်လီနောကုမ္ပဏီသည် တယ်လီနောမြန်မာလီမိတက်ကို ရောင်းချခြင်းဖြင့် မြန်မာနိုင်ငံမှ လုပ်ငန်းရပ်တန့်ထွက်ခွာရာတွင် နိုင်ငံစုံစီးပွားရေးလုပ်ငန်းများအတွက် OECD လမ်းညွှန်ချက်များတွင် ပါဝင်သည့် အကြံပြုချက်များကို လိုက်နာရန် ပျက်ကွက်ခဲ့ကြောင်း အခိုင်အမာပြောဆိုခဲ့သည်။[1]

၂၀၂၂ ခုနှစ်၊ နွေလိုင်လတွင် သဘောတူခဲ့သည့် နားလည်မှုစာချွန်လွှာ (MOU)[2] အရ တိုင်ကြားချက်တွင် ပါဝင်သူများသည် ဆက်သွယ်ရေးနှင့် ပတ်သက်ပြီး မြန်မာနိုင်ငံတွင် ဆက်သွယ်ရေးဆိုင်ရာ အချက်အလက်နှင့် ပစ္စည်းကိရိယာများနှင့်၊ ၎င်းတို့မှတဆင့်အန္တရာယ်များ မည်သို့ဖြစ်ပေါ်လာနိုင်သည်တို့ အပါအဝင် ဒစ်ဂျစ်တယ်ခြေရာများ (ဒစ်ဂျစ်တယ် ပစ္စည်းများနှင့် ဝန်ဆောင်မှုများ အသုံးပြုစဉ်ချန်ရစ်ထားနိုင်သည့် အချက်အလက်များ - digital footprints) နှင့် စောင့်ကြပ်ကြည့်ရှုခြင်းဆိုင်ရာ အန္တရာယ်များကို နားလည်သဘောပေါက်နိုင်စေရန် လွတ်လပ်သော သတင်းအချက်အလက်နှင့် ဆက်သွယ်ရေးနည်းပညာ (အိုင်စီတီ) ဂေဟစနစ်လေ့လာမှုကို ပူးတွဲလုပ်ဆောင်ခဲ့သည်။ ဤလေ့လာမှု၏ နယ်ပယ်တွင် အစိုးရများမှ ကျူးလွန်သော အခြား ဒစ်ဂျစ်တယ်ဝန်ဆောင်မှုများအား အလွဲသုံးစားလုပ်ခြင်း၊ ဥပမာ - သတင်းမှား ဖြန့်ဝေခြင်း သို့မဟုတ် သတင်းအချက်အလက်ရယူခွင့်ကို ကန့်သတ်ပိတ်ပင်ခြင်းတို့ကို ပါဝင်ထည့်သွင်းထားခြင်းမရှိပါ။

ဤလေ့လာမှု အပြည့်အစုံသည် ပါဝင်သူများမှလွဲ၍ အပြင်သို့ဝေမျှမှုမရှိသေးပါ။ ဤလေ့လာမှုမှာ ၂၀၂၃ ခုနှစ်၊ ဇွန်လမှ ဒီဇင်ဘာလအတွင်း အများပြည်သူ ရရှိနိုင်သော အစီရင်ခံစာများ၊ စိစစ်လေ့လာချက်များ၊ အွန်လိုင်းမှ ရရှိနိုင်သော အရင်းအမြစ်များနှင့် အရပ်ဘက်လူမှုအဖွဲ့အစည်းများ၊ ပညာရှင်များ၊ နိုင်ငံတကာအဖွဲ့အစည်းများနှင့် အိုင်စီတီကဏ္ဍတို့မှ ကိုယ်စားလှယ်များနှင့် ပြုလုပ်ထားသော အင်တာဗျူးပေါင်း ၂၀ ခန့်အပေါ် အခြေခံထားပါသည်။ ဤသည်မှာ လေ့လာမှု၏ အများပြည်သူဆိုင်ရာ အနှစ်ချုပ် အစီရင်ခံစာဖြစ်သည်။

အစိုးရ၏ စောင့်ကြည့်မှုနှင့် ဒစ်ဂျစ်တယ်ခြေရာများနှင့်ပတ်သက်သည့် အကြောင်းအရာသည် မြန်မာနိုင်ငံကဲ့သို့ ပဋိပက္ခကြောင့် သက်ရောက်မှုခံစားရသည့် နေရာများ နှင့် အန္တရာယ်ရှိသော နယ်မြေ များ (CAHRAs)[i] တွင် ထိရှလွယ်မှုများ ဖြစ်စေနိုင်သည်။ လေ့လာမှုတစ်ခုလုံး၏ ဤလူထုအနှစ်ချုပ်အစီရင်ခံစာကို တင်ပြရန် အရေးကြီးသော်လည်း၊ မြန်မာနိုင်ငံရှိ သီးခြားအခြေအနေများနှင့် ပတ်သက်သော အသေးစိတ်အချက်များအပြင် မတူညီသော စောင့်ကြပ်ကြည့်ရှုခြင်းနည်းလမ်းများ၏ ဖော်ပြချက်များကို ဤအစီရင်ခံစာတွင် မပါဝင်ပါ။

[i] ဤအစီရင်ခံစာတစ်လျှောက်လုံးတွင် အသုံးပြုသည့် ပဋိပက္ခကြောင့် သက်ရောက်မှု ခံစားရသည့်နေရာများနှင့် အန္တရာယ်ရှိသောနယ်မြေများ (CAHRAs) ဟူသော ဝေါဟာရကို ဥပမာအားဖြင့် OECD Due Diligence Guidance ၊ UNDP and UN Human Rights Working Group Heightened Human Rights Due Diligence for Business in Conflict-Affected Contexts: A Guide နှင့် ပဋိပက္ခကြောင့် သက်ရောက်မှု ခံစားရသည့်နေရာများနှင့် အန္တရာယ်ရှိသောနယ်မြေများ ဖော်ထုတ်ခြင်းဆိုင်ရာ European Commission အကြံပြုချက်များ မှ ရှင်းလင်းချက်များနှင့် အဓိပ္ပါယ်ဖွင့်ဆိုချက်များအပေါ် အခြေခံ၍ ကျယ်ပြန့်စွာ အဓိပ္ပာယ်ကောက်ယူသင့်သည်။

ဒစ်ဂျစ်တယ်စောင့်ကြပ်ကြည့်ရှုခြင်း၏ လူ့အခွင့်အရေးဆိုင်ရာ သက်ရောက်မှုများ

Global Network Initiative (GNI) နှင့် Business for Social Responsibility (BSR) တို့၏ Across the Stack Tool "Human Rights Due Diligence Across the Technology Ecosystem"[3] သည် နည်းပညာကဏ္ဍ၏ ဂေဟစနစ်တွင် လုပ်ဆောင်နေသော မတူညီသော ပါဝင်သူများနှင့် ဂေဟစနစ်၏ အစိတ်အပိုင်းတစ်ခုစီနှင့် အသက်ဆိုင်ဆုံးသော အဆင့်မြင့်မားသည့် လူ့အခွင့်အရေးဆိုင်ရာ ပြဿနာများကို ခြုံငုံသုံးသပ်ဖော်ပြထားပါသည်။ အထူးသဖြင့် ပဋိပက္ခကြောင့် သက်ရောက်မှု ခံစားရသည့်နေရာများနှင့် အန္တရာယ်ရှိသောနယ်မြေများ (CAHRAs) တွင် ဒစ်ဂျစ်တယ်စောင့်ကြည့်မှုမှ လူတစ်ဦးချင်းစီ၏ လူ့အခွင့်အရေးအပေါ် သက်ရောက်မှုများမှာ အလွန်ပြင်းထန်နိုင်ပြီး အခြားပါဝင်သည်မှာ-

> ဆက်သွယ်ရေးတွင်ဖြစ်စေ၊ ဆက်ဆံရေးတွင်ဖြစ်စေ၊ ထင်မြင်ယူဆချက်များ သို့မဟုတ် အိမ်တွင်ဖြစ်စေ ပုဂ္ဂိုလ်ဆိုင်ရာလွတ်လပ်ခွင့်ကို ချိုးဖောက်ခြင်းသို့ ဦးတည်စေနိုင်သည့် စောင့်ကြပ်ကြည့်ရှုခြင်း၊

> လွတ်လပ်စွာ ထုတ်ဖော်ပြောဆိုခွင့်နှင့် လွတ်လပ်စွာ အသင်းအဖွဲ့နှင့် လွတ်လပ်စွာ လှုပ်ရှားသွားလာခွင့်အပေါ် တားဆီးကန့်သတ်သည့် သက်ရောက်မှုရှိစေပြီး ထုတ်ဖော်ပြောဆိုမှု၊ ထင်မြင်ယူဆမှု၊ ဘာသာရေး ကျင့်ထုံးများနှင့် ဆန္ဒပြမှုများတွင် ပါဝင်ခြင်းတို့တွင် မိမိကိုယ်ကို ဆင်ဆာဖြတ်တောက်ခြင်း (self-censorship) ကို ဖြစ်ပေါ်စေခြင်း၊

> မတရားဖမ်းဆီးချုပ်နှောင်ခြင်း၊ ညှဉ်းပန်းနှိပ်စက်ခြင်း၊ လူမဆန်စွာ နှိမ့်ချဆက်ဆံခြင်း၊ တရားမဲ့သတ်ဖြတ်ခြင်းသို့ ဦးတည်စေနိုင်သော စောင့်ကြည့်ခြင်း၊

> တိုင်းရင်းသားလူနည်းစုများကို အတင်းအဓမ္မလုပ်အားပေး စေခိုင်းခြင်း အပါအဝင် ခွဲခြားဆက်ဆံမှုကို တွန်းအားပေးသည့် စောင့်ကြပ်ကြည့်ရှုခြင်း- စသည်တို့ပါဝင်သည်။[4]

လူ့အခွင့်အရေးဆိုင်ရာ မဟာမင်းကြီးရုံး (OHCHR) ၏အဆိုအရ ၂၀၂၁ ခုနှစ် ဖေဖော်ဝါရီလမှစ၍ အာဏာသိမ်းပြီးကတည်းက "မြန်မာနိုင်ငံတွင် အဆုံးမရှိဘဲ၊ ဆက်တိုက်မြင့်မားနေသည်ဟု ယူဆရသည့် စစ်ရေးအကြမ်းဖက်မှုများသည် မြန်မာနိုင်ငံရှိ ဘဝကဏ္ဍအားလုံးကို လွှမ်းခြုံထားသည်။ [...] စစ်တပ်က ၎င်းတို့၏အာဏာနှင့် ဆန့်ကျင်သည့် လူတစ်ဦးချင်းစီနှင့် များစွာသော ပြည်သူလူထုအပေါ် အကြမ်းဖက်မှုကို ခွဲခြမ်းစိတ်ဖြာရာတွင် တိုက်ခိုက်မှု အကြိမ်ရေအမျိုးအစား၊ ပြင်းထန်မှုနှင့် ရက်စက်ကြမ်းကြုတ်မှုတို့ ဆက်တိုက်တိုးမြင့်လာသည်ကို သက်သေပြခဲ့သည်။"[5]

စစ်အာဏာရှင်တို့ အသုံးပြုသောလက်နက်တစ်ခုမှာ ဒစ်ဂျစ်တယ် စောင့်ကြည့်မှု ဖြစ်သည်။ စစ်အာဏာရှင်ကို ဆန့်ကျင်သည့်သူများကို ဥပမာအားဖြင့် စစ်အာဏာရှင်ကို ဝေဖန်သည့် အကြောင်းအရာများ အများသူငှာ ပို့စ်များနှင့် ထိုပို့စ်များကို မျှဝေခြင်းမှတဆင့်[6] ၊ ၎င်းတို့၏ ငွေကြေးလွှဲပြောင်းမှုများကို စောင့်ကြည့်ခြင်း[7] ၊ စစ်ဆေးရေးဂိတ်များတွင် သိမ်းဆည်းရမိသော မိုဘိုင်းဖုန်းစက်ပစ္စည်းများတွင် တွေ့ရှိရသည့် သတင်းအချက်အလက်များ[8] ၊ ဆန္ဒပြမှုများ[9] နှင့် ကျပန်းစစ်ဆေးခြင်းများ[10] မှတဆင့် ဖော်ထုတ်တွေ့ရှိခဲ့ကြောင်း ကျယ်ကျယ်ပြန့်ပြန့် ထုတ်ပြန်ကြေညာထားသည်။

Freedom House ၏ 'Freedom on the Net 2023' အစီရင်ခံစာတွင် ဤအခြေအနေများသည် အဆိုးရွားဆုံးအခြေအနေများတွင် ဖမ်းဆီးခြင်း၊ ထောင်ချခြင်း၊ ညှဉ်းပန်းနှိပ်စက်ခြင်းနှင့် သေဆုံးခြင်းတို့ မည်သို့ဖြစ်စေကြောင်း ဖော်ပြထားပါသည်။[11]

၂။ မတူညီသော ဒစ်ဂျစ်တယ်ဆိုင်ရာ ပါဝင်သူများနှင့် ၎င်းတို့စုဆောင်းကောက်ယူသော အချက်အလက်များ

လူတစ်ဦးချင်းစီ၏ ဒစ်ဂျစ်တယ်ခြေရာများကို မတူညီသော အဖွဲ့အစည်းများစွာမှ စုဆောင်း၊ သိမ်းဆည်း၊ မျှဝေအသုံးပြုထားသည့် ပုဂ္ဂိုလ်ဆိုင်ရာ အချက်အလက်များဖြင့် ပြုလုပ်ဖွဲ့စည်းထားသည်။ အိုင်စီတီဂေဟစနစ်ရှိ မတူညီသော ပါဝင်သူများသည် ၎င်းတို့၏ ဝယ်ယူသူများနှင့် အသုံးပြုသူများ၏ ပုဂ္ဂိုလ်ဆိုင်ရာ အချက်အလက်များကို စုဆောင်းခြင်းနှင့်/သို့မဟုတ် အခြားအဖွဲ့အစည်းများမှ ပုဂ္ဂိုလ်ဆိုင်ရာ အချက်အလက်များကို စုဆောင်း၊ သိမ်းဆည်း၊ မျှဝေရန်နှင့် အသုံးပြုရန်အတွက် အသုံးပြုနိုင်သည့် နည်းပညာကို ပံ့ပိုးပေးရာတွင် ပါဝင်နေသည်။[ii] ထိုပါဝင်သူများမှာ-

- ဆက်သွယ်ရေးနှင့် အင်တာနက် ဝန်ဆောင်မှုပေးသူများ၊
- ဆိုရှယ်မီဒီယာ ပလက်ဖောင်းများနှင့် အသုံးပြုသူထုတ်လုပ်ထားသော အကြောင်းအရာများ (content) ကိုခွင့်ပြုသည့် အခြားဝန်ဆောင်မှုများ၊
- စာတိုပေးပို့ခြင်း၊ (ပစ္စည်း) ပေးပို့ခြင်း၊ အင်္ဂါယာဉ် အက်ပ်များ၊ ဂိမ်းဆော့ခြင်း၊ စာရိုက်နိုင်သည့် ကီးဘုတ် အက်ပ်နှင့် လျှဒါန်းခြင်း ပြုလုပ်နိုင်သော အက်ပ်များ၊
- ဝန်ဆောင်မှုတစ်ခုအနေဖြင့် အခြေခံအဆောက်အအုံ၊ ပလက်ဖောင်းနှင့် ဆော့ဖ်ဝဲလ်ကို ပံ့ပိုးပေးသည့် cloud ဝန်ဆောင်မှုပေးသူများ၊
- ဘဏ်များ၊ ဆက်သွယ်ရေးလုပ်ငန်းများ (သို့) အခြား/အမီခိုကင်းသော အဖွဲ့အစည်းများမှ အကောင်အထည်ဖော်ထားသည့် ဒစ်ဂျစ်တယ် ငွေပေးချေမှု ပလက်ဖောင်းများ၊[12]
- စောင့်ကြည့်မှုဆိုင်ရာ နည်းပညာ (ကွန်ပျူတာဆိုင်ရာ ကိရိယာပစ္စည်းများ (hardware)၊ ဆော့ဖ်ဝဲလ်၊ ဝန်ဆောင်မှုများ) ကို စောင့်ကြည့်ထောက်လှမ်းခြင်းသော ရည်ရွယ်ချက်နှင့်/သို့မဟုတ် စောင့်ကြည့်ခြင်း ရည်ရွယ်ချက်အတွက် အလွဲသုံးစားလုပ်နိုင်ရန် အလားအလာရှိသည့် ပံ့ပိုးပေးသူများ။ ၎င်းတွင် CCTV ကိရိယာများနှင့် စနစ်များကို ပံ့ပိုးပေးသူများ၊ ဆက်သွယ်ရေးကွန်ရက်ဆိုင်ရာ ကိရိယာများနှင့် စီမံခန့်ခွဲသော

[ii] Global Network Initiative (GNI) နှင့် Business for Social Responsibility (BSR) တို့၏ Across the Stack Tool "Human Rights Due Diligence Across the Technology Ecosystem" သည် နည်းပညာဂေဟစနစ်တွင် ပါဝင်လုပ်ဆောင်နေသော မတူညီသော ပါဝင်သူများ၏ အဆင့်မြင့်မားသော လူ့အခွင့်အရေးဆိုင်ရာ ပြဿနာများနှင့် ဂေဟစနစ်၏ အစိတ်အပိုင်းတစ်ခုစီရှိ ကုမ္ပဏီများမှ ထည့်သွင်းစဉ်းစားသင့်သည့် အလေးဂရုပြု လုပ်ဆောင်ရမည့် မေးခွန်းများ ခြုံငုံသုံးသပ်ချက်ကို ဖော်ပြထားသည်။

ဝန်ဆောင်မှုများ၊ ဥပဒေနှင့်အညီ ကြားဖြတ်ရယူ၍ ဖြေရှင်းနည်းများ၊ spyware နှင့် စက်ပစ္စည်းဆိုင်ရာ မှုခင်းစစ်ဆေးခြင်းပညာ (device forensics)၊ နှင့် ဒရုန်းများ ပံ့ပိုးပေးသူများ ပါဝင်သည်။

<u>မြန်မာနိုင်ငံတွင် ဆက်သွယ်မှုနှင့် အင်တာနက်အသုံးပြုမှုဆိုင်ရာ အဓိကအချက်များ</u>

၂၀၂၃ ခုနှစ် ဇန်နဝါရီလအထိ မြန်မာနိုင်ငံတွင်[13]

- အင်တာနက်အသုံးပြုသူလူဦးရေ ၂၃.၉၃ သန်းရှိပြီး ယင်းသည် အင်တာနက်ထိုးဖောက်ပျံနှုန်းမှနှုန်း ၄၄ ရာခိုင်နှုန်း ရှိသည်နှင့် ညီမျှသည်။
- မိုဘိုင်းဖုန်း ချိတ်ဆက်ဆက်သွယ်မှုမှာ ၆၄.၆ သန်းရှိပြီး မိုဘိုင်း ထိုးဖောက်ပျံနှုန်းမှနှုန်း ၁၁၈.၈ ရာခိုင်နှုန်း ရှိသည်နှင့် ညီမျှကာ ဆက်သွယ်ရေးကွန်ယက်တစ်ခုထက် ပိုမိုသည့် အသုံးပြုမှုကို လူများစွာ အသုံးပြုနေသည်။
- မိုဘိုင်းဖုန်း ချိတ်ဆက်ဆက်သွယ်မှုများ၏ ၉၀.၃ ရာခိုင်နှုန်းသည် (3G၊ 4G၊ 5G) Broadband ချိတ်ဆက်မှု ဖြစ်သည်။
- ဒေတာ 1GB ကုန်ကျစရိတ်မှာ $၁.၁၁ ဒေါ်လာ ကုန်ကျပြီး ယင်းသည် ပျမ်းမျှဝင်ငွေ၏ ၁.၁၇ ရာခိုင်နှုန်းနှင့် ညီမျှသည်။
- Web traffic ၏ ၃၃ ရာခိုင်နှုန်းသည် လက်ပ်တော့နှင့် ကွန်ပျူတာမှဖြစ်၍ ၆၇ ရာခိုင်နှုန်း သည် မိုဘိုင်းဖုန်းမှဖြစ်ပြီး၊ ၉၀ ရာခိုင်နှုန်း သည် Android စက်ပစ္စည်းများမှ အစပြုပါသည်။
- အသက် ၁၅ နှစ်အထက်ရှိသည့် ၂၉ ရာခိုင်နှုန်းသည် မိုဘိုင်းငွေအကောင့်တစ်ခုရှိပြီး၊ ၃၆ ရာခိုင်နှုန်းသည် ငွေကြေးအဖွဲ့အစည်းတစ်ခုဖြင့် အကောင့်တစ်ခုရှိနေသည်။

၂၀၂၃ ခုနှစ် အောက်တိုဘာလတွင် Facebook အသုံးပြုသူ ၂၁ သန်းကျော်၊ Instagram အသုံးပြုသူ ၂ သန်းနီးပါးနှင့် Messenger အသုံးပြုသူ သန်း ၂၀ နီးပါးရှိသည်။[14]

ပုဂ္ဂိုလ်ဆိုင်ရာ အချက်အလက်များကို စုဆောင်းခြင်း၊ ထိန်းသိမ်းခြင်း၊ မျှဝေခြင်း နှင့် အသုံးပြုခြင်းတို့ ပြုလုပ်သည့် အခြားသော လုပ်ငန်းများစွာလည်းရှိပြီး (စောင့်ကြည့်ရေး ရည်ရွယ်ချက်များအတွက် နိုင်ငံအာဏာပိုင်များမှ ဝင်ရောက်နိုင်သည့် အလားအလာနှင့်အတူ) လူတစ်ဦးချင်းစီ၏ ဒစ်ဂျစ်တယ်ခြေရာများလည်း ပါဝင်သည်။ အသုံးပြုသူများ ကိုယ်တိုင်ကလည်း ၎င်းတို့၏ ကိုယ်ပိုင် ပို့စ်များ၊ like ပြုလုပ်ခြင်းများ၊ မှတ်ချက်များ၊ tag တွဲခြင်းများနှင့် အခြား အသုံးပြုသူမှ ထုတ်ပေးသော အကြောင်းအရာ (content) တို့ကို public domain (အများပြည်သူပိုင်နေရာ) တွင် ပုဂ္ဂိုလ်ဆိုင်ရာ အချက်အလက်များကို တိုက်ရိုက်ထည့်သွင်းလိုက်ပြီး ထိုအချက်အလက်များကို အာဏာပိုင်များမှ open-source intelligence (OSINT) မှတဆင့် စုဆောင်းနိုင်သည်။

အိုင်စီတီဂေဟစနစ်တွင် ပါဝင်သူအများစုသည် စီးပွားရေးလုပ်ငန်း ရည်ရွယ်ချက်များအတွက် ပုဂ္ဂိုလ်ဆိုင်ရာ အချက်အလက်များ (personal data) ကို ပုံမှန်စုဆောင်းခြင်း၊ သိမ်းဆည်းခြင်း၊ အသုံးပြုခြင်းနှင့် မျှဝေခြင်း နှင့်/သို့မဟုတ် တရားဝင်လုပ်ဆောင်ရန် လိုအပ်ပါက အများသူငှာရရှိနိုင်သော ပုဂ္ဂိုလ်ဆိုင်ရာအချက်အလက် မူဝါဒများ

(privacy policies) တွင် စီးပွားရေးလုပ်ငန်းရှင်များက ၎င်းတို့ကောက်ယူသည့် ပုဂ္ဂိုလ်ဆိုင်ရာ အချက်အလက်အချို့ကို အနည်းဆုံး ဖော်ပြပေးသည်။ ကုမ္ပဏီတစ်ခု၏ ပုဂ္ဂိုလ်ဆိုင်ရာ အချက်အလက်များကို ထိန်းသိမ်းထားသည့် ကြာချိန်သည် ကုမ္ပဏီ၊ နိုင်ငံနှင့် အချက်အလက် အမျိုးအစားအလိုက် သိသိသာသာကွဲပြားနိုင်ပြီး၊ ဥပမာ - Ranking Digital Rights သုတေသန မှ တွေ့မြင်နိုင်သကဲ့သို့ ဤအလေ့အကျင့်များနှင့် ပတ်သက်ပြီး ကုမ္ပဏီ၏ ပွင့်လင်းမြင်သာမှုပေါ်တွင်လည်း ကွဲပြားနိုင်သည်။[15]

ဤလေ့လာမှုအတွက် အင်တာဗျူးမေးမြန်းခံရသူများသည် မြန်မာနိုင်ငံတွင် အထူးသတိထားဖွယ်ရှိပြီး အန္တရာယ်မြင့်မားသော အချက်အလက်အမျိုးအစားအချို့ကို တညီတညွတ်တည်း ဖြေကြားခဲ့သည်။ ၎င်းတို့မှာ-

> အချိန်နှင့်တပြေးညီ တည်နေရာပြအချက်အလက်၊

> ဇီဝဆိုင်ရာ (biometric) အချက်အလက် နှင့်

> နိုင်ငံအတွင်း ရုပ်ပိုင်းဆိုင်ရာ တည်ရှိမှု (ဥပမာ- အခြေခံအဆောက်အအုံ၊ ရုံးများနှင့် ဝန်ထမ်းများ) ရှိသည့် ကုမ္ပဏီများမှ ရရှိသိမ်းဆည်းထားသော အချက်အလက်များသည် တရားစီရင်ရေးဆိုင်ရာ ထည့်သွင်းစဉ်းစားမှုများကြောင့် စစ်အစိုးရအနေနှင့် ယင်းအချက်အလက်များကို ရယူနိုင်ရန် တောင်းဆိုမှုတွင် အားသာသည့် အခြေအနေကောင်းများရှိနေသည်။

၃။ ဒစ်ဂျစ်တယ် ခြေရာများ (ဒစ်ဂျစ်တယ် ပစ္စည်းများနှင့် ဝန်ဆောင်မှုများ အသုံးပြုစဉ် ချန်ရစ်ထားနိုင်သည့် အချက်အလက်များ - digital footprints) အား စောင့်ကြပ်ကြည့်ရှုခြင်း

မြန်မာနိုင်ငံတွင် အာဏာသိမ်းပြီး မကြာမီတပ်မတော်မှ "လွတ်လပ်စွာ ထုတ်ဖော်ပြောဆိုခွင့်ကို တားဆီးပိတ်ပင်ရန် ဥပဒေမူဘောင်ကို တဖက်သတ် ပြင်ဆင်ပြီး ပြဋ္ဌာန်းခြင်း၊ တရားမျှတသော တရားစီရင်မှုဆိုင်ရာ အခွင့်အရေးများကို ငြင်းပယ်ခြင်းနှင့် ထောင်နှင့်ချီသည့် တက်ကြွလှုပ်ရှားသူများ၊ သတင်းသမားများနှင့် လူ့အခွင့်အရေး ကာကွယ်သူများအပေါ် မျှတသည့် တရားရင်ဆိုင်ခွင့် အခြေအနေများ ငြင်းပယ်ခံရခြင်းများ ဖြစ်ပေါ်ခဲ့သည်" ဟု ကုလသမဂ္ဂ လူ့အခွင့်အရေးဆိုင်ရာ မဟာမင်းကြီးရုံး (OHCHR) က ဖော်ပြခဲ့သည်။[16] ၂၀၂၄ ခုနှစ်တွင် လွတ်လပ်စွာ ထုတ်ဖော်ပြောဆိုခွင့်နှင့် ပုဂ္ဂိုလ်ဆိုင်ရာ လွတ်လပ်ခွင့်တို့ကို ပုံစံမျိုးစုံဖြင့် ချိုးဖောက်နိုင်မှုအား ဥပဒေအောက်တွင် တရားမျှတစွာ ဆောင်ရွက်နေဟန် ဖြစ်စေရေးအတွက် စောင့်ကြည့်ရေးဆိုင်ရာ ဥပဒေများတွင် ဖွင့်ဆိုရန် ကျန်ပြန့်ပြီး တိကျရှင်းလင်းသင့် ကန့်သတ်ချက်များအား ဖယ်ကြဉ်ထားသည်။[17]

မြန်မာနိုင်ငံတွင် ဒစ်ဂျစ်တယ်စောင့်ကြည့်ကြည့်ရှုခြင်းနှင့် ဆက်စပ်၍ အောက်ပါတို့ကို ဤလေ့လာမှုက ဖော်ထုတ်ခဲ့သည်-

- ဥပဒေနှင့်အညီ ကြားဖြတ်ရယူခြင်း (Lawful Intercept – LI) လုပ်နိုင်စွမ်းသည် အနည်းဆုံး မိုဘိုင်းဆက်သွယ်ရေးလုပ်ငန်းရှင် လေးခု၏ ဆက်သွယ်ရေးကွန်ရက်များတွင် လုပ်ဆောင်နိုင်သည်ဟု ယူဆရမည်။[18] ဆိုလိုသည်မှာ ဥပမာအားဖြင့်- မိုဘိုင်းတယ်လီဖုန်းခေါ်ဆိုမှုများ[iii]၊ မက်ဆေ့ချ်စာများ၊ သတင်းအချက်အလက်ကြားဖြတ်ရယူခြင်းဆိုင်ရာ (interception related information - IRI)[iv], နှင့် (ဆဲလ်တာဝါ ID ဖြင့်) စက်ပစ္စည်းတည်နေရာတို့ကို အချိန်နှင့်တပြေးညီ ကြားဖြတ်ရယူနိုင်သည်ဟု ဆိုလိုသည်။ မြန်မာနိုင်ငံတွင် မကြာခဏပြတ်တောက်ခံရနိုင်သည့် အင်တာနက်ဝန်ဆောင်မှုများကို ပိတ်ပစ်ခြင်းသည် လူများအား 2G ဆက်သွယ်ရေးကို မှီခိုအားထားရန် တွန်းအားပေးကာ ဥပဒေနှင့်အညီ ကြားဖြတ်ရယူခြင်း (LI) မှ စောင့်ကြည့်ခြင်းမှ အန္တရာယ်များကို တိုးပွားစေသည်။[19] LI သည် အချို့သော အခြေအနေများတွင် roaming traffic ကို ကြားဖြတ်ရယူရန်အတွက်လည်း အသုံးပြုနိုင်သည်ကို သတိပြုရန် အရေးကြီးသည်။ ထိုသို့သော အခြေအနေမျိုးမှာ ပြည်ပတွင် မြန်မာဆင်းကတ်ကို အသုံးပြု၍ မြန်မာနိုင်ငံရှိ ဖုန်းနံပါတ်တစ်ခုခေါ်ဆိုခြင်းနှင့်၊ မြန်မာနိုင်ငံရှိ နိုင်ငံခြားဆင်းကတ်အသုံးပြုသူတစ်ဦး၏ ပြည်တွင်းနံပါတ်ကို မြန်မာနိုင်ငံတွင် ခေါ်ဆိုခြင်း တို့ဖြစ်သည်။ ဖုန်းခေါ်ဆိုမှုများကို VoLTE[v] ဖြင့်ပြုလုပ်ပါက (မြန်မာ ဆက်သွယ်ရေးလုပ်ငန်း အော်ပရေတာနှင့် နိုင်ငံခြား ဆက်သွယ်ရေးလုပ်ငန်း အော်ပရေတာတွင် VoLTE roaming လုပ်ခြင်းသဘောတူညီချက်တစ်ခု ရှိလျှင်) ဖုန်းခေါ်ဆိုမှုအားလုံးကို ကြားဖြတ်ရယူနိုင်ခြေရှိသည်။

- စစ်အာဏာရှင်က မိုဘိုင်းဆက်သွယ်ရေး အော်ပရေတာများထံမှ သိမ်းစည်းထားသော အသုံးပြုမှုမှတ်တမ်းများ (historical data)[20] ၊ ဥပမာအားဖြင့် subscription data၊ ဖုန်းခေါ်ဆိုမှု အသေးစိတ်မှတ်တမ်း (call detail records - CDR)[vi] နှင့် တည်နေရာအချက်အလက်တို့နှင့် သက်ဆိုင်သည့် အချက်အလက်တို့ကို တောင်းခံထားကြောင်း သိရှိရသည်။ ၎င်းအချက်အလက်များနှင့် အခြားအသုံးပြုသူ၏ အချက်အလက်အမျိုးအစားများကိုလည်း ပြည်တွင်း၌ လည်ပတ်နေသော ဒစ်ဂျစ်တယ်ဘဏ်လုပ်ငန်း (digital banking) ဝန်ဆောင်မှုများ၊ VPN သို့မဟုတ် မြန်မာကီးဘုတ်အက်ပ်များကဲ့သို့သော အခြား ဒစ်ဂျစ်တယ် ဝန်ဆောင်မှုများမှလည်း တောင်းဆိုခြင်း သို့မဟုတ် ဝင်ရောက်ကြည့်ရှုသည်ဟု ယူဆသင့်သည်။[21]

[iii] မှတ်ချက်- WhatsApp သို့မဟုတ် Signal ကဲ့သို့ စာတိုပေးပို့သည့် အက်ပ်များကဲ့သို့သော Voice-over-IP (VoIP) မပါဝင်ပါ။

[iv] ကြားဖြတ်ရယူခြင်းဆိုင်ရာ အချက်အလက် (IRI) တွင် အသံခေါ်ဆိုမှုတစ်ခု၏ ဦးတည်ရာ (ဥပမာ- တစ်စုံတစ်ယောက်၏ ခေါ်ဆိုသည့် ဖုန်းနံပါတ်)၊ ခေါ်ဆိုမှု၏ အရင်းအမြစ် (ခေါ်ဆိုသူ၏ ဖုန်းနံပါတ်)၊ ခေါ်ဆိုထားသည့် အချိန်နှင့် ကြာချိန်တို့အပါအဝင် ပစ်မှတ်ထားသော ဆက်သွယ်ရေးဆိုင်ရာ အချက်အလက်များ ပါဝင်ပါသည်။

[v] LTE သည် Long Term Evolution သို့မဟုတ် 4G ကို ကိုယ်စားပြုသည်။ 4G/LTE ကွန်ရက်များသည် ဒေတာများကိုသာ သယ်ဆောင်ပြီး Voice over IP / Voice over LTE (VoLTE) အဖြစ် အသံဖြင့် ထုတ်လွှင့်ပါသည်။

[vi] ဖုန်းခေါ်ဆိုမှု အသေးစိတ်မှတ်တမ်းများ (CDRs) များသည် အရင်းအမြစ်နံပါတ်နှင့် ဦးတည်ရာနံပါတ်၊ အချိန်၊ ကြာချိန်၊ routing ၊ cell ID (ခေါ်ဆိုမှုချိတ်ဆက်ထားသည့် အခြေစိုက်စခန်း) နှင့် ဖုန်းခေါ်ဆိုမှုတို့၏ ပြီးဆုံးသည့်အခြေအနေ နှင့် စာတိုပေးပို့မှုများ (ဖုန်းကျသွားသော ခေါ်ဆိုမှုများ) နှင့် ပုံမှန်အားဖြင့် ဒါဇင်ပေါင်းများစွာသော အသုံးပြုမှုနှင့် ရှာဖွေရေးအချက်အလက်များ ကဲ့သို့သော မိုဘိုင်းတယ်လီဖုန်းခေါ်ဆိုမှု သို့မဟုတ် စာတိုမက်ဆေ့ချ် (SMS) ၏ရည်ညွှန်းချက်များဖြစ်သည်။ IRI နှင့်ဆန့်ကျင်ဘက်အနေနှင့် CDR သည် သိမ်းစည်းထားသော အသုံးပြုမှုမှတ်တမ်း အချက်အလက်ဖြစ်ပြီး ဥပဒေနှင့်အညီ ကြားဖြတ်ရယူခြင်းမရှိဘဲ ရနိုင်သည်။

- မိုဘိုင်း ငွေလွှဲပြောင်းမှုများအပါအဝင် ဒစ်ဂျစ်တယ် ငွေကြေးလွှဲပြောင်းမှုများကို စောင့်ကြည့်နေပြီး ဘဏ်လုပ်ငန်းနှင့် ငွေပေးချေမှု ပလက်ဖောင်းအသစ် Know-Your-Customer (KYC) လိုအပ်ချက်တို့သည် လူတစ်ဦးချင်းစီကို ခြေရာခံနိုင်သည်ဟု ဆိုလိုသည်။[22]
- စစ်အာဏာရှင်သည် ရည်ရွယ်ချက်ဖြင့် တည်ဆောက်ထားသော OSINT ကိရိယာများ[23] ကို အသုံးပြုနိုင်ကာ အများပြည်သူ၏ ဆိုရှယ်မီဒီယာ လှုပ်ရှားမှုများကို စဉ်ဆက်မပြတ် စောင့်ကြည့်နေသည့် အလားအလာရှိပြီး သီးသန့် ပရိုဖိုင်များ (private profiles) နှင့် အဖွဲ့များသို့ ဝင်ရောက်ကြည့်ရှုမှုများ အထူးသဖြင့် Facebook နှင့် Telegram ကဲ့သို့သော နာမည်ကြီး အပလီကေးရှင်းများအား စောင့်ကြည့်မှုများတွင် သတင်းပေးသူများကို မှီခိုနေသည်။[24]
- စစ်အစိုးရသည် သိမ်းဆည်းခံထားသည့် စက်ပစ္စည်းကိရိယာများပေါ်တွင် မှုခင်းဆေးပညာဆိုင်ရာ spyware များကို အသုံးပြုနေကြောင်း ခိုင်လုံသော အစီရင်ခံစာများ ရှိနေသည်။[25] ဆိုလိုသည်မှာ စက်ပစ္စည်းတွင်ရှိနေသည့် အကြောင်းအရာများနှင့် ဖျက်လိုက်သည့်အကြောင်းအရာများသည်ပင် ပြန်လည်ရယူနိုင်ခြေရှိသည်။ အခြားသူများထံမှ အချက်အလက် စုဆောင်းရန်အတွက် စက်ပစ္စည်းပိုင်ရှင်များကဲ့သို့ အယောင်ဆောင်ရန်အတွက်လည်း ဤအချက်အလက်ကို အသုံးပြုနိုင်သည်။
- စစ်အာဏာရှင်သည် အဆိုပါ စက်ပစ္စည်းများတွင် လုပ်ဆောင်မှုအားလုံးကို ဝင်ရောက်နိုင်ပြီး ၎င်းတို့အနီးတစ်ဝိုက်ရှိ လုပ်ဆောင်မှုအားလုံးကို ဝင်ရောက်နိုင်သည့် spyware ဖြင့်အဝေးမှ စက်ပစ္စည်းများကို ကူးစက်နိုင်ရန် ကိရိယာများ လက်ဝယ်ရှိကြောင်း ညွှန်ပြချက်များရှိသည်။[26] ၎င်းသည် ပြည်ပရောက် မြန်မာတက်ကြွလှုပ်ရှားသူများအတွက် အန္တရာယ်လည်း ဖြစ်စေသည်။

ဤစောင့်ကြပ်ကြည့်ရှုရေးနည်းလမ်းများကို မည်ကဲ့သို့ ကျယ်ကျယ်ပြန့်ပြန့်နှင့် စနစ်တကျ အသုံးပြုနေကြောင်း၊ နိုင်ငံတော် စီမံအုပ်ချုပ်ရေးကောင်စီ (SAC) ၏ မည်သည့်အဖွဲ့များက၊ သို့မဟုတ် မည်သို့အခြေအနေအထိ လုပ်နိုင်သည်ကို အတိအကျသိရှိရန်မှာ စိန်ခေါ်မှုတစ်ခုဖြစ်သည်။ ၂၀၂၃ ခုနှစ်တွင် မြန်မာစစ်အစိုးရက ဆင်းကတ်မှတ်ပုံတင်ရာတွင် အသုံးပြုနိုင်သည့် အီလက်ထရောနစ် ID (eID)[27] ကို စတင်ပြုလုပ်ရန်အတွက် လူဦးရေသန်းခေါင်စာရင်း စီမံချက်အတွင်းနှင့် ပြင်ပတွင် ဇီဝမှတ်တမ်းဆိုင်ရာ အချက်အလက် (biometric data) စုဆောင်းမှုကို အရှိန်မြှင့်လုပ်ဆောင်ခဲ့သည်။[28] စစ်အာဏာရှင်သည် အိန္ဒိယ 'Aadhaar' eID စနစ်ကို စတင်ကျင့်သုံးခြင်းအကြောင်းကို အိန္ဒိယအစိုးရနှင့် ဆွေးနွေးမှုများ၊[29] နိုင်ငံသားစိစစ်ရေးကတ်များကို eID စမတ်ကတ်များဖြင့် အစားထိုးခြင်းနှင့် ပတ်သက်ပြီး တရုတ်အရာရှိများနှင့်လည်း ဆွေးနွေးမှုများ ပြုလုပ်ခဲ့သည်။[30] ဤလုပ်ဆောင်မှုများသည် နိုင်ငံတစ်ဝှမ်းတွင် CCTV များ ဆက်တိုက်တပ်ဆင်လာမှုနှင့်အတူ[31] ပိုမိုခေတ်မီသော စောင့်ကြည့်ရေးစနစ်တစ်ခု ထားရှိရန် အစီအစဉ်များကို ညွှန်ပြနိုင်သည်။ စစ်အာဏာရှင်ကို ခုခံရန် ခိုင်ခိုင်မာမာ ဆုံးဖြတ်ချက်ချထားပြီး[32] များပြားသော အချိန်၊ ငွေနှင့် အရင်းအမြစ်များ လိုအပ်နေမည့် မြန်မာနိုင်ငံအခြေအနေတွင် ၎င်းသည် ရိုးရှင်းသောအလုပ် မဟုတ်ပေ။

၄။ အန္တရာယ်လျော့ပါးခြင်းနှင့် ပြန်လည်ကုစားမှုပေးခြင်း

ကုလသမဂ္ဂ လူ့အခွင့်အရေးဆိုင်ရာ မဟာမင်းကြီးရုံး (OHCHR) မှ ပစ်မှတ်ထား၍စောင့်ကြည့်ခြင်းခံရသူများသည် ထိခိုက်မှုများကို ပြန်လည်ကုစားပေးရန်နေနေသာသာ ထိခိုက်နစ်နာမှုအား အသိအမှတ်ပြုမှုရရှိရန်ပင် မအောင်မြင်ကြောင်း မှတ်ချက်ပြုထားသည်။[33] အိုင်စီတီကဏ္ဍအတွင်းရှိ ပြန်လည်ကုစားခြင်းနှင့် စပ်လျဉ်းသည့် အထူးစိန်ခေါ်မှုများကို ကုလသမဂ္ဂ၏ စီးပွားရေးနှင့် လူ့အခွင့်အရေးများဆိုင်ရာ လမ်းညွှန်အခြေခံမူများနှင့် ကိုက်ညီသော ပြန်လည်ကုစားနည်းကို လေ့လာခဲ့သည့် OHCHR ၏ B-Tech စီမံကိန်း၏ လုပ်ငန်းဆောင်ရွက်မှုမှ အသိအမှတ်ပြုခံရပါသည်။ သီးခြား အိုင်စီတီကုမ္ပဏီတစ်ခု၏ နည်းပညာ သို့မဟုတ် လုပ်ဆောင်ချက်များနှင့် ထိခိုက်မှုရှိသော ကိစ္စရပ်တစ်ခုကို ချိတ်ဆက်ရန် စိန်ခေါ်မှုအပြင် B-Tech မှ နည်းပညာကုမ္ပဏီများသည် "မတူညီသော နည်းပညာများကို အသုံးပြုသည့် နည်းလမ်းများအကြောင်း အသိပညာပေးခြင်း၊ [... နှင့်] မတူညီသော ဒီဇိုင်း သွင်ပြင်လက္ခဏာများ (features) ၏ လူ့အခွင့်အရေးဆိုင်ရာ သက်ရောက်မှုများအကြောင်း အများပြည်သူများနှင့် ပွင့်လင်းမြင်သာစွာပြုလုပ်ခြင်း" ဖြင့် "ထိခိုက်မှုကိုခံရသူများ၊ အုပ်စုများနှင့် ၎င်းတို့၏ ကိုယ်စားလှယ်များကို ခွန်အားပေးခြင်းဖြင့် ပြန်လည်ကုစားပေးသည့် ဂေဟစနစ်များ၏ လုပ်ငန်းဆောင်တာများကို မြှင့်တင်နိုင်သည်" ဟု အကြံပြုထားသည်။[34]

လေ့လာမှု၏ ရည်ရွယ်ချက်များထဲမှ တစ်ခုသည် 'ဒစ်ဂျစ်တယ်လုံခြုံရေးဆိုင်ရာ ကယ်ဆယ်ရေး လုပ်ငန်းယန္တရား' ကို စူးစမ်းလေ့လာရာတွင် ထည့်သွင်းပေးရန် နှင့် အထူးသဖြင့် အဆိုပါယန္တရားက အန္တရာယ်များကို လျော့ပါးစေရန်အတွက် ပါဝင်နိုင်သည့် အခန်းကဏ္ဍကို ထည့်သွင်းဖော်ပြပေးခြင်း ဖြစ်သည်။ 'ဒစ်ဂျစ်တယ်လုံခြုံရေးဆိုင်ရာ ကယ်ဆယ်ရေး လုပ်ငန်းယန္တရား' သည် ဒစ်ဂျစ်တယ်ခြေရာများနှင့် ပတ်သက်သော အန္တရာယ်များကို လျှော့ချရန်အတွက် အဓိကထားသည့် ရန်ပုံငွေတစ်မျိုးမျိုးကို ဆိုလိုကြောင်း နားလည်သိမှတ်ထားသည်။

ဤလေ့လာမှုအတွက် အင်တာဗျူးတွင် မေးမြန်းခံရသူများသည် ထိုသို့သော လုပ်ငန်းယန္တရားက ပေးစွမ်းနိုင်သည့်အရာအပေါ် အမြင်အမျိုးမျိုးရှိကြသည်။ လူ့အခွင့်အရေး ကာကွယ်သူများ (HRDs) သည် ဒစ်ဂျစ်တယ်ခြေရာများ၏ အန္တရာယ်များနှင့် ၎င်းတို့၏ ဘေးကင်းလုံခြုံရေးအတွက် အန္တရာယ်များကို လျှော့ချရန် လုပ်ဆောင်နိုင်သည့် အချက်များ ပိုမိုသိရှိနားလည်သော်လည်း များစွာသော နည်းပညာပိုင်းဆိုင်ရာ အကာအကွယ်များကို အသုံးပြုနိုင်ရန် အရင်းအမြစ်များ နည်းပါးနေပါသည်။ လူအများအပြားအတွက် ပိုမိုကောင်းမွန်သော ဒစ်ဂျစ်တယ်လုံခြုံရေးဆိုင်ရာ အသိပညာပေးရန်အတွက်လည်း များစွာလိုအပ်ပါသည်။ အင်တာဗျူးတွင် မေးမြန်းခံရသူများသည် ပြည်တွင်းပြည်ပရှိ မြန်မာ လူ့အခွင့်အရေး ကာကွယ်သူများ၊ သတင်းထောက်များနှင့် ပညာရှင်များ၏ လုပ်ငန်းများကို ပံ့ပိုးကူညီရန် အရင်းအမြစ်များ လိုအပ်ကြောင်း ထုတ်ဖော်ပြောဆိုခဲ့သည်။

မြန်မာနိုင်ငံတွင် ဒစ်ဂျစ်တယ်လုံခြုံရေးဆိုင်ရာ ကယ်ဆယ်ရေး လုပ်ငန်းယန္တရားကို အကောင်အထည်ဖော်ရာတွင် လက်တွေ့ကျသော စိန်ခေါ်မှုများ ရှိနေပြီး ထိုစိန်ခေါ်မှုများအနက်မှ မှန်ကန်သော ပံ့ပိုးကူညီမှုကို မှန်ကန်သော

လူတစ်ဦးချင်းနှင့် အဖွဲ့များထံ ရောက်ရှိစေရန်၊ ၎င်းတို့နှင့် အခြားသူများ ကြုံတွေ့ရနိုင်သည့် အန္တရာယ်များကို တိုးမြှင့်ခြင်းမရှိဘဲ၊ သေချာအောင်ပြုလုပ်ခြင်းတို့ ပါဝင်သည်။

၅။ အကြံပြုချက်များ

ဤလေ့လာမှုမှ အောက်ပါ အကြံပြုချက်များ ဖော်ပြပါသည်။

အိုင်စီတီကုမ္ပဏီအားလုံးအတွက်

> ကုလသမဂ္ဂ၏ စီးပွားရေးနှင့် လူ့အခွင့်အရေးများဆိုင်ရာ လမ်းညွှန်အခြေခံမူများ အပါအဝင် နိုင်ငံတကာ အသိအမှတ်ပြုသော ဥပဒေများနှင့် လူ့အခွင့်အရေးစံနှုန်းများအပေါ် အခြေခံ၍ ခိုင်မာသော မူဝါဒများနှင့် စနစ်များကို ထူထောင်ပါ။ ယင်းတို့သည် အိုင်စီတီဂေဟစနစ်ရှိ မတူညီသော ပါဝင်သူများ ရှိကြသည့် မတူညီသော အခန်းကဏ္ဍများ၊ တာဝန်များနှင့် အကျိုးသက်ရောက်မှုများနှင့် အလားအလာရှိသော ထိခိုက်မှုများ လျော့ပါးအောင် ဆောင်ရွက်သည့် စီမံချက်များ ထင်ဟပ်ပြသစေသင့်သည်။ ဥပမာအားဖြင့် စောင့်ကြပ်ကြည့်ရှုရေး နည်းပညာကို ပံ့ပိုးပေးသူများသည် ၎င်းတို့၏ ထုတ်ကုန်များကို အစိုးရများက အလွဲသုံးစားမလုပ်ကြောင်း သေချာစေရန်အတွက် မူဝါဒများနှင့် စနစ်များကို ချမှတ်သင့်သည် (သို့မဟုတ်) အစိုးရများထံမှ တောင်းဆိုချက်များကို တုံ့ပြန်ရာတွင် ဆက်သွယ်ရေးနှင့် အင်တာနက် ဝန်ဆောင်မှုပေးသူများက အကောင်အထည်ဖော် လုပ်ဆောင်သင့်သည့် မူဝါဒများနှင့် စနစ်များ ကွဲပြားနေသည်။

> အထက်ပါအချက်များနှင့် ဆက်စပ်၍ အိုင်စီတီကုမ္ပဏီများအတွက် ပုဂ္ဂိုလ်ဆိုင်ရာ လွတ်လပ်ခွင့် (privacy) နှင့် စောင့်ကြည့်ရေး နှင့် ပတ်သက်၍ အလေးဂရုပြုလုပ်ဆောင်ရမည့် လမ်းညွှန်ချက်များ ဖြစ်ပေါ်လာစေနိုင်သည့် အခွင့်အလမ်းတစ်ခုလည်း ဖြစ်သည်။ ဤလမ်းညွှန်ချက်သည် မတူညီသော အန္တရာယ်များ၊ သက်ရောက်မှုများ၊ တာဝန်ရှိမှုများနှင့် ထိခိုက်မှု လျော့ပါးအောင် ပြုလုပ်သည့် စီမံချက်များကို အသေးစိတ် စီစဉ်ချမှတ်နိုင်ပြီး အိုင်စီတီဂေဟစနစ်ရှိ မတူညီသော ပါဝင်သက်ဆိုင်သူများအတွက် ကောင်းမွန်သောအလေ့အကျင့်များကို ဖော်ထုတ်နိုင်ပါသည်။

> နိုင်ငံတွင်း လူ့အခွင့်အရေးဆိုင်ရာ သက်ရောက်မှု အကဲဖြတ်စိစစ်ချက်များကို နိုင်ငံအတွင်းမှ အခွင့်အရေးကိုင်ဆောင်သူများ၏ ရှုထောင့်များနှင့် ကျွမ်းကျင်မှုများဖြင့် အသိပေးခြင်းဖြစ်အောင် သေချာစွာ ပြုလုပ်ပါ။

> လူ့အခွင့်အရေးများ လေးစားမှုရှိရေးအတွက် အလေးဂရုပြုလုပ်ဆောင်မှုများ (HRDD) လုပ်ငန်းစဉ်မှ တွေ့ရှိချက်များနှင့် ထိုတွေ့ရှိချက်များမှ ဖော်ပြသည့် အန္တရာယ်များ တားဆီးလျော့ပါးစေရန် ဆောင်ရွက်သည့် လုပ်ဆောင်ချက်များကိုလည်း ပွင့်လင်းမြင်သာစွာ ပြောဆိုဖော်ပြပါ။

- ကုမ္ပဏီမှ ကောက်ယူစုဆောင်းသည့် (သက်ဆိုင်ရာ နိုင်ငံအဆင့်ရှိ အချက်အလက်သိမ်းဆည်းသည့် ကာလများ အပါအဝင်) ပုဂ္ဂိုလ်ဆိုင်ရာ အချက်အလက်များ နှင့် ဤအချက်အလက်များကို အာဏာပိုင်များနှင့် မည်သို့မျှဝေနိုင်သည်တို့ကို အသုံးပြုသူများအား အသေးစိတ် ဖော်ပြပေးပါ။ အချက်အလက်စုဆောင်းမှု၊ နည်းပညာ၊ စောင့်ကြပ်ကြည့်ရှုရေး လုပ်ငန်းယန္တရားများနှင့် ယင်းတို့ မည်သို့ ပေါ်ပေါက်လာနိုင်သည်တို့ကို အရပ်ဘက်လူမှုအဖွဲ့အစည်းများမှ ပါဝင်သက်ဆိုင်သူများ သိရှိနားလည်လာအောင် ပံ့ပိုးကူညီပါ။

- သက်ဆိုင်သူများက ၎င်းတို့၏ အိုင်စီတီအသုံးပြုမှုနှင့် ပတ်သက်၍ သိရှိနားလည်မှုအပေါ် အခြေခံပြီး ဆုံးဖြတ်ချက်များ ပိုမိုချမှတ်နိုင်စေရန် ကိန်းဂဏန်းအစီရင်ခံစာ ဖော်ပြရုံသာမက ဝယ်ယူသူ/အသုံးပြုသူ၏ အချက်အလက်များကို အာဏာပိုင်တို့မှ တောင်းဆိုမှုများနှင့်စပ်လျဉ်းသည့် ဆက်စပ်အချက်အလက်များကို ပံ့ပိုးဖော်ပြပေးပါ။.[35]

- မည်သူက မည်သို့ စောင့်ကြည့်မှုကို လုပ်ပိုင်ခွင့်ရှိနိုင်သည်၊ မည်သို့သော ကျဉ်းမြောင်းစွာ သတ်မှတ်ထားသည့် အခြေအနေများတွင်၊ လွတ်လပ်သော ကြီးကြပ်ကွပ်ကဲမှုဖြင့် ပြုလုပ်နိုင်သည် စသည်တို့နှင့်ပတ်သက်၍ ရှင်းရှင်းလင်းလင်း ဖော်ပြသည့် အခွင့်အရေးများ လေးစားလိုက်နာသော ဥပဒေများ ပေါ်ပေါက်လာစေရန်အတွက် အားပေးတိုက်တွန်းလုပ်ဆောင်ပါ။

- အထူးသဖြင့် ပဋိပက္ခကြောင့် သက်ရောက်မှု ခံစားရသည့်နေရာများ နှင့် အန္တရာယ်ရှိသော ဒေသများ၌ စျေးကွက်ဝင်ရောက်မှုတွင် ပြုလုပ်ခဲ့သော လူ့အခွင့်အရေးသက်ရောက်မှုများ လေ့လာဆန်းစစ်ခြင်း (human rights impact assessments) ၏ တစ်စိတ်တစ်ပိုင်းအနေဖြင့် ဖြစ်နိုင်ချေရှိသော နိုင်ငံမှ လုပ်ငန်းရပ်တန့်စွန့်ခွာမှု၏ လူ့အခွင့်အရေးသက်ရောက်မှုများကို သေချာစွာ ထည့်သွင်းစဉ်းစားမှု ပြုလုပ်ပါ။ ၎င်းလေ့လာဆန်းစစ်ခြင်းတွင် အနာဂတ်၌ ဖြစ်နိုင်ခြေရှိသော လုပ်ငန်းရပ်တန့်စွန့်ခွာမှု၏ ထိခိုက်မှုများကို လျှော့ချရန် ခွဲခြားသတ်မှတ်ထားသည့် အဆင့်များ ပါဝင်သင့်သည်။ (ဥပမာ- data minimisation (စုဆောင်းထားသည့် အချက်အလက်ကို သက်ဆိုင်ရာနှင့် လိုအပ်သည့်အရာများသာ ကောက်ယူသည်အထိ လျှော့ချခြင်း))။

- ပဋိပက္ခကြောင့် သက်ရောက်မှု ခံစားရသည့်နေရာများနှင့် အန္တရာယ်ရှိသောနယ်မြေများတွင်ရှိသော လုပ်ငန်းစဉ်များကို အဓိကအာရုံစိုက်၍ ကုမ္ပဏီ၏ အကျပ်အတည်းစီမံခန့်ခွဲမှု (crisis management) အစီအမံနှင့် ပုံမှန်အကျပ်အတည်း လေ့ကျင့်ရေးတို့တွင် လူ့အခွင့်အရေးဆိုင်ရာ ထည့်သွင်းစဉ်းစားမှုများနှင့် လုပ်ငန်းရပ်တန့်စွန့်ခွာမှု အခြေအနေများကို ထည့်သွင်းပါ။

- ရှုပ်ထွေးပြီး လျင်မြန်စွာ ပြောင်းလဲနေသော အခြေအနေများအတွက် ပဋိပက္ခကြောင့် သက်ရောက်မှု ခံစားရသည့်နေရာများနှင့် အန္တရာယ်ရှိသောနယ်မြေများတွင် မြန်ဆန်သော လူ့အခွင့်အရေးများ လေးစားလိုက်နာမှုရှိရေးအတွက် အလေးဂရုပြုလုပ်ဆောင်မှုများ (human rights due diligence - HRDD) အတွက် လုပ်ငန်းစဉ်များကို စီစဉ်ခြင်းနှင့် အန္တရာယ်ကျရောက်နိုင်ပြီး ထိခိုက်လွယ်သော အခွင့်အရေးကိုင်ဆောင်သူအများစုကို ဖော်ထုတ်သတ်မှတ်ခြင်း အပါအဝင် ၎င်းနယ်မြေများအတွင်းရှိ

လုပ်ငန်းဆောင်ရွက်မှုများနှင့် စပ်လျဉ်း၍ အင်တိုက်အားတိုက် တက်တက်ကြွကြွဖြင့် မြှင့်တင်ထားသော HRDD ကို လုပ်ဆောင်ပါ။

> ကုမ္ပဏီက အသုံးပြုသူများ၏ ဒစ်ဂျစ်တယ်ဘေးကင်းရေးနှင့် လုံခြုံရေးနှင့် သက်ဆိုင်သည့် ယေဘုယျနည်းလမ်းများနှင့် ပဋိပက္ခကြောင့် သက်ရောက်မှု ခံစားရသည့်နေရာများနှင့် အန္တရာယ်ရှိသောနယ်မြေများရှိ အသုံးပြုသူများ ရင်ဆိုင်နေရသော သီးခြားအခြေအနေများနှင့် ဆက်စပ်၍ ကူညီပံ့ပိုးပေးနိုင်သည့် နည်းလမ်းများကို မြန်မြန်ဆန်ဆန် ဖော်ထုတ်ပါ။ ဥပမာ-

    - ဒစ်ဂျစ်တယ်ဘေးကင်းရေးနှင့် လုံခြုံရေးကို ပံ့ပိုးပေးသည့် ဝန်ဆောင်မှုများနှင့် သွင်ပြင်လက္ခဏာများ (features) ကို ကမ်းလှမ်းပေးခြင်း (ဥပမာ Nord VPN ၏ အခမဲ့ အရေးပေါ် VPN ကမ်းလှမ်းချက်[36] နှင့် အသုံးပြုသူများက ၎င်းတို့၏ profile ကို လျင်မြန်လွယ်ကူစွာ လော့ခ်ချနိုင်စေမည့် Facebook ၏ လုံခြုံရေး feature[37])၊
    - ထုတ်ကုန်နှင့် ဝန်ဆောင်မှုအသစ်များအတွက် လုံခြုံမှုရှိသော ဒီဇိုင်း (security-by-design) လုပ်ငန်းစဉ်များ တည်ဆောက်ခြင်း (နိုင်ငံအတွင်းရှိ သီးသန့်အခြေအနေနှင့် အန္တရာယ်များကို ထည့်သွင်းစဉ်းစားခြင်းဖြင့်)၊
    - အသုံးပြုသူများကြားတွင်၊ အထူးသဖြင့် အကြီးမားဆုံးသော အန္တရာယ်သက်ရောက်နိုင်မှုရှိနိုင်သည့် အခွင့်အရေးကိုင်ဆောင်ထားသူများမှ၊ ဒစ်ဂျစ်တယ်ဘေးကင်းရေးနှင့် လုံခြုံရေး သိရှိနားလည်မှု တည်ဆောက်ရန် ပိုမိုကျယ်ပြန့်သော ပဏာမခြေလှမ်းများကို ပံ့ပိုးကူညီခြင်း၊
    - အိုင်စီတီကိုအသုံးပြု၍ လူ့အခွင့်အရေးချိုးဖောက်မှုများကို မီးမောင်းထိုးပြရန်နှင့် ပိုမိုသိရှိနားလည်လာစေရန် လုပ်ဆောင်နေသော အရပ်ဘက်လူမှုအဖွဲ့အစည်းများနှင့် ပညာရပ်ဆိုင်ရာ သုတေသနပြုမှုများကို ငွေကြေးထောက်ပံ့ပေးခြင်းနှင့် ပစ္စည်းပံ့ပိုးပေးခြင်း၊
    - ထိခိုက်လွယ်သောသူများအား ကုမ္ပဏီနှင့် လုံခြုံစွာ ဆက်သွယ်ပြောဆိုဆက်ဆံနိုင်ရန် နှင့် လူတစ်ဦးချင်းစီအတွက် ပြန်လည်ကုစားပေးရေး ရရှိနိုင်ရန် လုပ်ငန်းဆောင်ရွက်မှုအဆင့်ရှိသည့် နစ်နာမှုများကို တိုင်ကြားနိုင်သည့် လုပ်ငန်းစဉ်များကို ထားရှိပါ။

တယ်လီနောအတွက်

သက်ဆိုင်သည့် အတိုင်းအတာအရ အထက်ဖော်ပြပါ အကြံပြုချက်များအားလုံးသည် တယ်လီနောအား အိုင်စီတီကုမ္ပဏီတစ်ခုအနေဖြင့် အကြံပြုထားခြင်းများလည်း ဖြစ်သည်။ ထို့အပြင်-

> မြန်မာနိုင်ငံမှ လုပ်ငန်းရပ်တန့်စွန့်ခွာမှုအကြောင်း လေ့လာမှု လုပ်ငန်းစဉ်မှ တွေ့ရှိချက်များကို ဆက်လက်အကောင်အထည်ဖော်ပြီး [38] ပွင့်လင်းမြင်သာစွာဖြင့် အောက်ပါအချက်များ မျှဝေပါ-

- ၎င်းလုပ်ငန်းစဉ်သည် ကုမ္ပဏီ၏မူဝါဒမူဘောင်နှင့် ဌာနတွင်းလုပ်ထုံးလုပ်နည်းများအပေါ် မည်သို့ သက်ရောက်မှုရှိပုံ နှင့် ထိုအပြောင်းအလဲများကို လက်ရှိလုပ်ငန်းဆောင်တာများတွင် မည်သို့ ပြုလုပ်ဆောင်ရွက်နေပုံ၊
- ကုမ္ပဏီသည် ၎င်း၏ အတွေ့အကြုံများနှင့် သင်ယူရရှိလာသည်များကို အခြားသူများအား မည်သို့ နှင့် မည်သည့်နေရာတွင် မျှဝေနေပုံ၊
- ဘုတ်အဖွဲ့ဝင်များအတွက် သင်တန်းပို့ချမှုနှင့်ပတ်သက်၍ ဆောင်ရွက်ဆဲ အခြေအနေ နှင့်
- ကုမ္ပဏီသည် အရပ်ဘက်လူမှုအဖွဲ့အစည်းများနှင့် ရင်းနှီးမြှုပ်နှံသူများနှင့် ချိတ်ဆက်ဆောင်ရွက်မှု တိုးတက်ပြောင်းလဲလာပုံ။

ပါဝင်သူများ (တယ်လီနော နှင့် တိုင်ကြားသူများ) အတွက်

> အနာဂတ် ဆွေးနွေးမှုများနှင့် အလားအလာရှိသော ဒစ်ဂျစ်တယ်လုံခြုံရေးဆိုင်ရာ ကယ်ဆယ်ရေး လုပ်ငန်းယန္တရား စူးစမ်းလေ့လာရေး စမ်းသပ်ချက်၏ တစ်စိတ်တစ်ပိုင်းအနေဖြင့် ယင်းလုပ်ငန်းယန္တရားနှင့် ဆက်စပ်သော အန္တရာယ်များ၊ လက်တွေ့ကျသော ဖြစ်နိုင်ချေများနှင့် အလားအလာရှိသော အုပ်ချုပ်မှုစနစ်ကို ထည့်သွင်းစဉ်းစားပါ။

> ပိုမိုကျယ်ပြန့်စွာ ပြန်လည်ကုစားပေးရန်အတွက် ပါဝင်သူများက အတူတကွဖြင့် (သို့မဟုတ်) ကိုယ်ပိုင် တသီးတခြားဖြင့် ပါဝင်ဆောင်ရွက်နိုင်သည့် အခန်းကဏ္ဍကို လေ့လာကြည့်ပါ။ အထူးသဖြင့်-

- ဤကိစ္စရပ်မှ သိရှိနားလည်ထားသော တာဝန်ယူမှုရှိသည့် လုပ်ငန်းရပ်တန့်စွန့်ခွာမှုအတွက် လမ်းညွှန်ချက် ဖြစ်ပေါ်လာအောင် ဆောင်ရွက်ခြင်း နှင့်
- အိုင်စီတီကဏ္ဍအတွင်း ယေဘုယ်အားဖြင့် ပြန်လည်ကုစားပေးရေးကို ထည့်သွင်းစဉ်းစားရန် အစုအဖွဲ့ပေါင်းစုံပါဝင်သည့် ပူးပေါင်းဆောင်ရွက်ခြင်း။

အရပ်ဘက်အဖွဲ့အစည်းများ၊ ပညာရှင်များနှင့် သုတေသနအဖွဲ့အစည်းများအတွက်

> အခွင့်အရေးများကို လေးစားလိုက်နာသည့် ဥပဒေမူဘောင်များအတွက် ဆက်လက်ထောက်ခံအားပေးပါ။ ဥပမာ၊ အထူးသဖြင့် spyware နှင့်သက်ဆိုင်သော စည်းမျဉ်းစည်းကမ်းသည် အစီရင်ခံစာပြင်ဆင်ရေးသားချိန်တွင် အဓိကဖြစ်သည်။[39]

> တက်ကြွလှုပ်ရှားသူများနှင့် လူ့အခွင့်အရေး ကာကွယ်သူများ (HRDs) အား ၎င်းတို့၏ နည်းပညာနှင့် ဒစ်ဂျစ်တယ် လုံခြုံရေး လေ့လာကျွမ်းကျင်ရန် လုံခြုံရေးသင်တန်းများ လိုအပ်ချက်များနှင့်အတူ အန္တရာယ်များမှ မိမိကိုယ်ကို ပိုမိုကောင်းမွန်စွာကာကွယ်နိုင်ရန် ကူညီပံ့ပိုးပေးပြီး အိုင်စီတီကုမ္ပဏီများနှင့်

ထိထိရောက်ရောက် ချိတ်ဆက် ဆောင်ရွက်ပြီး ကုမ္ပဏီများ တာဝန်ယူမှု၊ တာဝန်ခံမှုရှိစေရန် ရည်ရွယ်ချက်ဖြင့် ဆက်လက် ပံ့ပိုးကူညီပါ။

> မြန်မာနိုင်ငံတွင် စစ်အစိုးရက အသုံးပြုနေသည့် စောင့်ကြည့်ထောက်လှမ်းရေးနည်းလမ်းများ၊ အထူးသဖြင့် တရားဝင်ကြားဖြတ်နားထောင်ခြင်း၊ CCTV စနစ်များနှင့် ပစ်မှတ်ထားသော spyware များကို အသုံးပြုခြင်းစသည့် စစ်အစိုးရတို့ အလိုရှိသလို အသုံးပြုနိုင်သော နည်းလမ်းများကို ပိုမိုနားလည်သိရှိလာစေရန်အတွက် သုတေသနပြုလုပ်မှုများအား အာရုံစိုက်၍ လုပ်ဆောင်ပါ။

> သုတေသနပြုလုပ်ရာတွင် ပိုမိုကျယ်ပြန့်စွာ ထည့်သွင်းစဉ်းစားနိုင်သည့် နယ်ပယ်နှစ်ခုမှာ- စောင့်ကြည့်ရေး ရည်ရွယ်ချက်အတွက် အချက်အလက်ရရှိနိုင်ရန် ပွဲစားများအသုံးပြုခြင်းနှင့် ပိုမိုခေတ်မီပြီး AI အခြေပြု စောင့်ကြည့်ရေးစနစ်များကို အသုံးပြုနိုင်စေရန် cloud ဝန်ဆောင်မှုများကို အလွဲသုံးစားပြုလုပ်ခြင်း တို့ဖြစ်သည်။

ဘက်ပေါင်းစုံပါသော အဖွဲ့အစည်းများနှင့် အစိုးရများအတွက်

> ပဋိပက္ခကြောင့် သက်ရောက်မှု ခံစားရသည့်နေရာများနှင့် အန္တရာယ်ရှိသောနယ်မြေများရှိ အစိုးရများအား အိုင်စီတီကဏ္ဍဆိုင်ရာ ဘဏ္ဍာရေးနှင့် ဖွံ့ဖြိုးတိုးတက်ရေးနှင့် သက်ဆိုင်သည့် ပံ့ပိုးကူညီမှုမှာ အခွင့်အရေးများကို လေးစားလိုက်နာသော ဥပဒေမူဘောင်များနှင့် ကြီးကြပ်မှုတို့ အကောင်အထည်ဖော်ရာတွင် အခြေအနေအရဖြစ်ကြောင်း သေချာအောင်ပြုလုပ်ပါ။

> ပဋိပက္ခကြောင့် သက်ရောက်မှု ခံစားရသည့်နေရာများနှင့် အန္တရာယ်ရှိသောနယ်မြေများတွင် အိုင်စီတီ အခြေခံအဆောက်အအုံ ဖွံ့ဖြိုးတိုးတက်မှု၊ ဥပမာ- ဒစ်ဂျစ်တယ် ID သို့မဟုတ် ဘဏ်လုပ်ငန်းစနစ်များ သို့မဟုတ် မှုခင်းကြိုတင်ကာကွယ်ရေး နည်းပညာများ လေ့ကျင့်ပေးခြင်း၊ စသည်တို့တွင် ငွေကြေးထောက်ပံ့ပေးခြင်းနှင့် ပစ္စည်းပံ့ပိုးပေးခြင်းတို့ ပြုလုပ်ရာတွင် လူ့အခွင့်အရေး အန္တရာယ်များနှင့် အကျိုးသက်ရောက်မှုများကို ထည့်သွင်းစဉ်းစားပါ။[40]

> လက်ရှိ ဒဏ်ခတ် ပိတ်ဆို့အရေးယူမှုများကို တင်းကြပ်စွာ ပြဋ္ဌာန်း၍ လုပ်ဆောင်ခြင်းအပြင် ရေတို၊ အလယ်အလတ်နှင့် ရေရှည် သက်ရောက်မှုများ မည်ကဲ့သို့ ပြောင်းလဲလာမည်ကို ထည့်သွင်းစဉ်းစားကာ ဒဏ်ခတ်ပိတ်ဆို့မှုများ၏ လူ့အခွင့်အရေးသက်ရောက်မှုများ လေ့လာဆန်းစစ်ခြင်းများ (human rights impact assessments) ပြုလုပ်ပါ။

> အိုင်စီတီနည်းပညာ အသုံးပြု၍ အာဏာရှင်နိုင်ငံများ၏ လူ့အခွင့်အရေးချိုးဖောက်မှုများကို မီးမောင်းထိုးပြရန်နှင့် သိရှိနားလည်လာစေရန် ဆောင်ရွက်နေသော အရပ်ဘက်လူ့အဖွဲ့အစည်းများ၊ လွတ်လပ်သော သတင်းပညာနှင့် ပညာရပ်ဆိုင်ရာ သုတေသနပြုလုပ်မှုများအား ငွေကြေးထောက်ပံ့မှုနှင့် ပစ္စည်းများ ကူညီပံ့ပိုးပေးပါ။

End Notes

[1] NCP Norway (2021): NCP accepts submission, offers good offices to the parties

[2] NCP Norway (2022): Update in specific instance – MoU

[3] BSR and the Global Network Initiative (2022): Human Rights Due Diligence Across the Technology Ecosystem

[4] Access Now, Business & Human Rights Resource Centre, and Heartland Initiative (2022): Navigating the surveillance technology ecosystem: A human rights due diligence guide for investors

[5] UN Human Rights Office of the High Commissioner (OHCHR) (2023): Situation of human rights in Myanmar - report

[6] Freedom House (2023): Freedom on the Net – Myanmar

[7] Radio Free Asia Myanmar (2023): Myanmar shutters 700 mobile bank accounts suspected of funding anti-junta forces

[8] Ibid. Freedom House (2023)

[9] Free Expression Myanmar (2020): No Permission to Protest

[10] Myanmar Centre for Responsible Business (2022): The Right to Privacy in the Digital Age: Experience from Myanmar

[11] Ibid. Freedom House (2023)

[12] Ei Nandar Kyaw, Myanmore (2022): The revolution of Myanmar fintech : mobile payment applications

[13] Datareportal (2023): Myanmar

[14] Social Media users in Myanmar - October 2023 | NapoleonCat (accessed in December 2023)

[15] The 2022 Ranking Digital Rights Telco Giants Scorecard and Ranking Digital Rights - The 2022 RDR Big Tech Scorecard – အထူးသဖြင့် မေးခွန်း P6.1 ကိုကြည့်ပါ။

[16] Ibid. OHCHR (2023)

[17]ဤလေ့လာမှုမှာ- ဆက်သွယ်ရေး ဥပဒေ (၂၀၁၃)၊ မူးယစ်ဆေးဝါးနှင့် စိတ်ကိုပြောင်းလဲစေသော ဆေးဝါးများဥပဒေ (၂၀၁၈)၊ အကြမ်းဖက်မှုတိုက်ဖျက်ရေးဥပဒေ (၂၀၂၃)၊ နိုင်ငံသားများ၏ ပုဂ္ဂိုလ်ဆိုင်ရာ လုံခြုံမှုနှင့် ပုဂ္ဂိုလ်ဆိုင်ရာလုံခြုံမှုကို ကာကွယ်ရေးဥပဒေ (၂၀၁၇)၊ အီလက်ထရောနစ်ဆက်သွယ်ဆောက်ရွက်ရေး ဥပဒေ (၂၀၂၁)၊ နှင့် ဆိုက်ဘာလုံခြုံရေး ဥပဒေ (၂၀၂၁) စသည်တို့တွင် ပါရှိသည့် အာဏာပိုင်များအား ပေးအပ်ထားသော အခွင့်အာဏာများကို လေ့လာသည်။ ဤဥပဒေများစွာကို လေ့လာသုံးသပ်ချက်များနှင့် ဘာသာပြန်ဆိုချက်များကို Free Expression Myanmar: ဥပဒေ မှ ရရှိနိုင်ပါသည်။

[18] Phyu Phyu Kyaw, Open Technology Fund (2020): The Rise of Online Censorship and Surveillance in Myanmar

[19] Myanmar Centre for Responsible Business (2022): Private Security Companies in Myanmar, and Interviews

[20] See Telenor: Handling access requests from authorities (accessed in October 2023)

[21] Ibid., Radio Free Asia Myanmar (2023)

[22] Frontier Myanmar (2022): Junta weaponises digital banking transition to starve resistance funding

[23] Intelligence Online (2022): Kremlin's favourite OSINT expert helps Russian plans in Myanmar

[24] Fanny Potkin and Wa Lone, Reuters (2021): Insight: 'Information combat': Inside the fight for Myanmar's soul and interviews

[25] International Crisis Group (2021): Myanmar's Military Struggles to Control the Virtual Battlefield

[26] Securelist by Kaspersky (2019): New FinSpy iOS and Android implants revealed ITW and interviews

[27] Myanmar Now (2023): Myanmar junta launches pilot census

[28] Ibid. MCRB (2022)

[29] Ministry of Information of Myanmar (2023): MoIP Union Minister seeks Myanmar-India cooperation in e-ID system

[30] Radio Free Asia (2023): Junta enlists China in changing Myanmar IDs to biometric smart cards

[31] Article 19 and Digital Rights Collective (2022): Who buys and controls the CCTV? Myanmar's slippery slope to mass surveillance

[32] Jonathan Head & Lulu Luo, BBC (2023): A turning point in Myanmar as army suffers big losses

[33] OHCHR (2019): Surveillance and human rights - Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, pp.12-13

[34] B-Tech (2021): Access to remedy and the technology sector: a "remedy ecosystem" approach, p. 6

[35] ကုမ္ပဏီများမှ ထုတ်ဖော်ပြန်ဝေသည်မှာ ဥပဒေဆိုင်ရာ ကန့်သတ်ချက်များ ရှိနိုင်သည်။ ဥပမာအားဖြင့် Global Network Initiative (GNI) ၏ Country Legal Frameworks Resource ကိုကြည့်ပါ။

[36] Nord VPN: Emergency VPN program

[37] Meta: Facebook Introduces a New Safety Feature in Myanmar

[38] Telenor (2023): Telenor publishes learning outcomes from Myanmar engagement

[39] European Parliament Press release (2023): Spyware: MEPs call for full investigations and safeguards to prevent abuse

[40] Michael Safi, The Guardian (2021): EU provided crowd control training to Myanmar police units; Brigitte Bureau, CBC (2020): Canada funding migrant-blocking operations in countries with poor human rights records; Access Now (2022): Open letter: World Bank and its donors must protect human rights in digital ID systems