Mr. Xavier Espot Zamora, Minister of Justice, Home and Social Affairs of Andorra

SESSION 1: ***Addressing Cybersecurity***

Mr. Xavier Espot Zamora, Minister of Justice, Home and Social Affairs of Andorra

Tuesday, 3 October 2017

Senyora presidenta,

Senyor secretari general,

Senyor síndic,

Senyor cap de Govern,

Distingides autoritats,

Senyores i senyors,

Els juristes de l'antiga Roma deien *ubi societas, ibi ius*: allà on hi ha una comunitat humana, hi ha normes jurídiques. Aquest adagi llatí es pot entendre com la descripció d'una realitat: allà on hi ha relacions humanes hi ha sempre algun tipus de norma; però també es pot entendre com la manifestació d'un desig: allà on hi ha una societat hi hauria d'haver normes que la regulessin. Fins i tot hi ha autors que allarguen la màxima llatina i diuen: *ubi societas, ibi ius, ibi litis*: allà on hi ha una comunitat humana, hi ha normes i també hi ha conflictes.

Les persones del nostre temps haurem tingut l'extraordinari privilegi de viure en directe el naixement d'un nou tipus de comunitat humana. Fins fa unes poques dècades el món havia conegut només societats en el sentit físic de la paraula: Comunitats nacionals i una comunitat internacional que s'ha anat fent cada vegada més forta. Nosaltres –les persones del nostre temps- hem vist néixer la societat virtual: Amb totes les noves oportunitats que obre i tots els nous problemes que crea. Hem vist néixer la societat virtual, estem entre tots treballant per tenir unes normes aplicables a aquesta societat virtual i estem assistint també a nous conflictes que tenen lloc en aquesta societat virtual.

La societat virtual s'ha anat construint al llarg dels últims 25 anys amb elements diversos: Des d'alguns aparentment senzills, com els correus electrònics, fins a transaccions online de tot tipus, com compravendes entre particulars o tràmits burocràtics oficials amb l'administració pública. Ara bé, la màxima expressió d'aquesta nova realitat són –sens dubte- les xarxes socials. Actualment, arreu del món, més de 1.500 milions de persones tenen un compte a Facebook, més de 1.000 milions utilitzen Whatsapp com a servei de missatgeria, uns 400 milions pengen les seves fotografies a Instagram, 320 milions de persones piulen a Twitter, 300 milions fan servir Skype, 250 milions són usuaris de Viber, 200 milions de Snapchat i 100 milions de persones tenen un perfil professional a Linkedin.

Aquesta nova comunitat virtual ha generat, de manera espontània, els seus propis llenguatges, els seus propis usos i costums i –en certa forma- les seves pròpies normes. Em sembla important remarcar això últim: Les xarxes socials en particular i la comunitat virtual en el seu conjunt generen de manera espontània les seves normes. Com també les societats humanes primigènies s'organitzaven de manera espontània. Aquí a Andorra en conservem un bon exemple: les nostres comunitats locals estan regides pels Comuns que, en origen, a l'Alta Edat Mitjana, van néixer com a institucions d'autogovern, creades pels mateixos pagesos d'Andorra per ordenar qüestions tan bàsiques com la tala dels boscos o l'ús de les pastures.

Les societat humanes –físiques o virtuals- creen les seves pròpies normes i codis de conducta i majoritàriament els respecten; sense necessitat d'un tercer extern, d'una mena de Leviatan, que obligui al compliment de les normes.

Em sembla important remarcar aquest punt perquè quan parlem de seguretat, de regulació i de prevenció i persecució dels crims, hem de tenir sempre present que la gran majoria de la gent fa un bon ús de les eines que la societat posa al seu abast. És sempre una minoria la que, ja sigui per imprudència o bé per voluntat de fer mal, trenca les normes i els codis de conducta.

És per això que quan parlem de seguretat hem de tenir sempre present la ponderació d'altres drets i béns jurídics que també mereixen protecció. Així com el principi de proporcionalitat a l'hora de garantir aquesta seguretat i combatre aquells que l'amenacen; perquè res no és tan contraproduent com matar mosques a canonades.

Tot i que la majoria de les persones compleixen de manera voluntària amb les normes –tan en la realitat física com en la realitat virtual-, el creixement exponencial que ha viscut la comunitat virtual en les últimes dècades ha anat acompanyat d'un creixement –també exponencial- de la cibercriminalitat.

Fa quatre anys, un article al rotatiu britànic *The Guardian* ens va fer prendre consciència de la realitat del cibercrim: Entre el 2008 i el 2012, al Regne Unit, les denúncies de crims comesos a les xarxes socials van créixer un 780%: De 556 denúncies el 2008 a 4.908 denúncies el 2012.

La proliferació de les xarxes socials ha anat acompanyada d'una proliferació de la cibercriminalitat. Però també m'agradaria fer notar un matís: Els índex de cibercriminalitat els obtenim –molt sovint- gràcies a les denúncies de les mateixes víctimes. Per tant, també podem dir que hi ha hagut una presa de consciència per part dels usuaris d'aquestes xarxes socials: Persones que fa 8 o 10 anys no tenien consciència de ser víctimes d'un crim per un ús il·lícit de les seves dades personals avui en tenen consciència.

Sigui com sigui, el grau d'exposició que tots nosaltres tenim a la cibercriminalitat és molt elevat: En el que portem de dia, en tot el món, ja hi ha hagut 800.000 persones que han estat víctimes d'un cibercrim. Això és el que es desprèn de les estadístiques: 1,2 milions de persones són víctimes de la cibercriminalitat cada dia; el que equival a 50.000 persones cada hora, 820 persones cada minut i 14 persones per segon. 7 de cada 10 persones hauran estat víctimes del cibercrim en algun moment de la seva vida, fins i tot persones que no són usuàries de xarxes socials.

Davant d'aquestes dades xocants ¿hauríem de concloure que la proliferació de les xarxes socials i de la comunitat virtual ha multiplicat la criminalitat? Seria una conclusió –al meu entendre- precipitada i mancada de matisos: Les noves tecnologies de la comunicació i la informació han multiplicat les interaccions humanes de tot tipus i és això el que ha obert nous espais, noves oportunitats i noves modalitats per a les conductes criminals.

Bona prova d'això que dic és que una gran majoria dels anomenats cibercrims són crims que ja existien i que ara es cometen utilitzant les noves tecnologies, especialment internet. Delictes com la difusió de continguts il·lícits (de pornografia infantil, o de racisme o antisemitisme), els fraus de tots tipus o els atemptats a la propietat intel·lectual o industrial (com còpies o falsificacions). Tots aquests delictes ja existien abans de l'eclosió d'internet i de les xarxes socials. I, per tant, en la majoria dels casos no s'ha requerit una adaptació legal per ser tipificats com a delictes.

El que sí ha estat necessari és canviar la manera en què perseguim i prevenim aquests delictes. Perquè l'espai digital obre noves arenes on es cometen aquests delictes i noves modalitats de comissió dels mateixos. I, si bé dificulta, en alguns casos, la investigació, també pot facilitar-la en altres casos. I, evidentment, també en l'àmbit d'internet cal sempre mesurar bé que la persecució i la prevenció de delictes no afecti de manera desmesurada béns jurídics mereixedors de protecció com la intimitat o les llibertats d'expressió i comunicació.

Ara bé, més enllà dels crims que ja existien –i estaven tipificats- amb anterioritat a l'existència d'internet, el creixement del ciberespai ha anat acompanyat de l'aparició d'un altre tipus d'infraccions penals, aquestes sí, nascudes en l'àmbit de les noves tecnologies. Quan parlem de violacions dels sistemes de tractaments automatitzats de dades, de virus informàtics que poden atacar i danyar aquests sistemes, de difusió de programes per clonar o crear falses targetes de crèdit, d'infraccions de les normes sobre criptologia o signatura electrònica, d'usurpació de la identitat digital... Estem assistint a l'aparició de nous tipus de delictes que només existeixen en el món virtual i que no existien abans de l'aparició d'aquesta nova realitat.

I aquí sí que ha calgut adaptar de manera constant la legislació penal per poder prevenir la realització o sancionar aquests tipus de conductes. En molts casos, per tipificar-les com a delicte.

Aquesta tasca de tipificació no és fàcil i comporta –sovint- més complicacions del que hom podria imaginar: Perquè el cibercrim qüestiona de ple un dels principis bàsics del dret penal tal i com el coneixíem fins ara: la territorialitat. Les conductes són delictives o no en funció del lloc on es cometen, és a dir, en funció de la llei penal que està en vigor al lloc on es cometen. En el cas del cibercrim, el concepte de lloc, d'indret, es difumina. Víctimes i agressors poden estar en indrets diversos, separats per milers de quilòmetres de distància, i amb ordenaments jurídics molt diferents. I això pot dificultar enormement la lluita contra aquests delictes.

Tampoc no és res nou: Abans de l'aparició d'internet, delictes com el tràfic de drogues, el blanqueig de capitals o el terrorisme -per posar només alguns exemples-, ja havien agafat una dimensió transnacional que superava clarament l'abast dels instruments clàssics de què disposaven els Estats-nació per combatre la criminalitat.

Ara bé, l'aparició de la cibercriminalitat ha estat el veritable punt d'inflexió en aquesta qüestió. Aquells 50.000 cibercrims que –segons les estadístiques- es produeixen cada hora al món requereixen en molts casos una resposta internacional coordinada. En aquest sentit, un dels passos més significatius fins a la data ha estat el Conveni del Consell d'Europa sobre la Cibercriminalitat –l'anomenat Conveni de Budapest- que ja ha estat ratificat per 55 països, entre ells Andorra.

El Conveni de Budapest és el primer instrument internacional vinculant per lluitar contra el cibercrim i el frau online; a més, posteriorment, mitjançant un Protocol addicional, s'hi ha afegit la lluita contra la propagació del racisme i la xenofòbia fent ús de les noves tecnologies. Un Conveni que, en aplicar-lo, incideix de ple en el dret penal material dels països amb la introducció de noves tipologies i modalitats de delictes.

Més enllà del cibercrim en el sentit estricte –és a dir, d'aquells crims que es cometen utilitzant internet- les noves tecnologies de la informació i la comunicació també tenen incidència en altres conductes delictives. En primer lloc, tenim el que podríem anomenar crims d'oportunitat, entesos com aquells delictes que no es cometen utilitzant internet, però en els quals els criminals obtenen informació a internet que facilita la comissió del delicte.

Els crims d'oportunitat són crims en què hi ha poc risc i molta recompensa. Un clar exemple seria entrar a robar a una casa buida, sabent que els seus habitants estan de viatge. El fet que hi hagi xarxes socials –com Facebook o Instagram- que permeten fer un check-in, també permet als potencials lladres saber quan les persones són o no a casa seva. Un altre exemple seria el d'assaltar, o segrestar o violar una persona en un indret solitari. Si pengem totes les nostres activitats a les xarxes socials, els criminals potencials poden conèixer i estudiar els nostres hàbits, els llocs on ens movem, les persones amb les quals ens trobem o les activitats que fem.

Per combatre els crims d'oportunitat que proliferen gràcies a l'ús d'internet i molt especialment de les xarxes socials, no cal modificar la legislació, sinó utilitzar l'educació com a eina fonamental per a la prevenció. Una bona educació de la ciutadania sobre els seus hàbits digitals és clau per evitar que augmentin els crims d'oportunitat vinculats a internet.

De fet, l'educació i la conscienciació de la població sobre els riscos que implica utilitzar de forma poc responsable les xarxes socials contribueix, no només a prevenir els crims d'oportunitat vinculats a internet, sinó també a prevenir tot tipus de cibercriminalitat.

La ciberseguretat i la criminalitat a internet tenen una altra vessant que tampoc no està directament vinculada amb el cibercrim: L'ús d'internet per part de criminals o organitzacions criminals amb finalitats de reclutament, propaganda o logística. No es tracta –en aquest cas- de cibercrim, de crims comesos en el ciberespai, sinó d'organitzacions criminals que utilitzen internet com un instrument més per preparar les seves activitats.

Un cas molt clar el trobem en el terrorisme. Les organitzacions terroristes utilitzen internet per reclutar membres, per promocionar les seves accions o per coordinar les seves activitats. Les noves tecnologies de la informació i la comunicació han esdevingut molt útils per a les noves modalitats de terrorisme, basades en cèl·lules autònomes que no requereixen grans quantitats de recursos ni una coordinació complexa.

I, en aquest àmbit, també s'estan fent avenços. S'hi ha referit el cap de Govern fa una estona, en el seu parlament inaugural: La darrera Assemblea General de Nacions Unides va ser l'escenari d'una declaració sobre la prevenció de l'ús d'internet per part dels terroristes, impulsada per un dels nostres coprínceps i alhora president de la República Francesa, Emmanuel Macron, la primera ministra del Regne Unit, Theresa May, i el president de torn del G7, el primer ministre italià, Paolo Gentiloni.

Més enllà de nombrosos caps d'Estat i de Govern i altres representants de la comunitat internacional, l'acte va aplegar també els representants de la indústria d'internet. I això posa de manifest una altra de les potes clau de la ciberseguretat: La necessitat d'implicar agents no governamentals. En aquest sentit, la declaració feta a Nova York el mes passat recull el compromís de grans empreses tecnològiques-com Google, Facebook, YouTube, Microsoft o Twitter- per remoure el material relacionat amb el terrorisme en un termini d'una o dues hores, per prevenir que aquest material pugui tornar a ser penjat a la xarxa i per desenvolupar eines tecnològiques que permetin lluitar contra el reclutament i la propaganda terroristes. A banda d'això, les companyies també es van comprometre a seguir aplicant i millorant codis de bones pràctiques respecte d'aquesta qüestió.

A més, les grans empreses tecnològiques també s'han compromès a ajudar empreses i plataformes més petites a desenvolupar i implementar mecanismes de prevenció, control i reacció. Perquè el microterrorisme que estem vivint no s'aprofiti de les microplataformes d'internet.

Aquest repàs que he fet sobre la cribercriminalitat i la relació del crim amb internet ens ha permès veure els que –al meu entendre- són els tres elements essencials de la ciberseguretat:

1. Abordar la qüestió des d'una perspectiva internacional: Cap país, per gran i poderós que sigui, no pot garantir per si sol la ciberseguretat dels seus ciutadans.
2. Educar la població en l'ús d'internet: Per entendre els riscos i les oportunitats que representa.
3. Involucrar agents no governamentals: des d'ONGs fins a empreses del sector tecnològic.

Aquests tres elements són claus per millorar la seguretat d'aquesta nova comunitat humana –ara ja no tant nova- que és internet. Però m'agradaria acabar aquesta intervenció reprenent una idea que he apuntat al principi: L'element més essencial per mantenir un ordre determinat és que la majoria de la població confiï i cregui en aquest ordre. I no podem oblidar que la gran majoria de transaccions i interaccions a internet són segures perquè la gran majoria de la població no fa un ús fraudulent o il·legal de les noves tecnologies.

Per tant, de res no serviria lluitar contra la cibercriminalitat si aquesta lluita acabés vulnerant la privacitat, la llibertat d'expressió o altres drets fonamentals de la majoria de la població que fa un ús correcte d'internet.

Nosaltres, que hem viscut el naixement i l'expansió de la comunitat virtual, podem dir amb coneixement de causa que l'ideal rousseaunià del bon salvatge no es correspon amb la realitat: Les persones abans

del món d'internet no eren millors que les persones en el món d'internet.

De fet, les mateixes tecnologies que serveixen a uns pocs per cometre delictes a la xarxa o utilitzant la xarxa, també serveixen a una majoria per coordinar-se davant dels delictes o dels abusos. Recentment, l'estiu passat, durant els atacs terroristes a Barcelona i Cambrils, vam poder veure com la comunicació a través de les xarxes socials es va convertir en un element clau per informar la població, per aconseguir que la gent seguís les recomanacions de seguretat, per coordinar l'ajuda als afectats i per facilitar la identificació i persecució dels terroristes.

I s'hi van implicar tots els agents necessaris: les administracions públiques, molt notablement la policia, i també entitats privades i nombrosos ciutadans individualment. Ciutadans que –sense cap tipus de mesura coercitiva- van complir amb les recomanacions de seguretat, van col·laborar amb la policia per difondre la informació necessària i no difondre la informació sensible per garantir l'èxit de la investigació, i es van auto-organitzar per ajudar les persones afectades pels atacs.

Per seguir avançant en la ciberseguretat ens cal, doncs, més dret internacional en la matèria; més educació a la població; una major implicació dels agents no governamentals; i una ciutadania conscient que la seguretat en el món virtual és tan important com la seguretat en el món físic.

Moltes gràcies.

Descarregueu el discurs