

## *Seguretat i privacitat per a periodistes, comunicadors i ciutadans*

Dates: 8 de febrer - 15 de març de 2018

Lloc: Hangar. Emilia Coranty, 16 - 08018 Barcelona

### **1. Presentació**

Les revelacions d'Edward Snowden han posat sobre la taula com els estats i companyies tecnològiques vigilen l'activitat d'usuaris de tot el món, i això ha contribuït a que la societat pugui visibilitzar i conscienciar-se sobre la importància de preservar la privacitat i la seguretat en les seves comunicacions. En termes generals, no es percep la importància ni la quantitat de dades que estem generant contínuament i, per tant, no sabem quines conseqüències poden tenir els rastres digitals que es produeixen a partir d'activitats quotidianes com donar un «like» a una publicació, enviar un mail o utilitzar els serveis i aplicacions «gratuïts».

Aquest tipus de qüestions afecten d'una manera singular a les persones que treballen com a informadors mentre que la privacitat de les comunicacions està estretament relacionada amb la llibertat d'expressió ja que aquesta és un prerrequisit essencial per poder exercir el dret a la informació. La manca de privacitat afecta directament la capacitat dels informadors i comunicadors en tant que propicia l'autocensura, ja que si saben o intueixen que estan sent observats, no parlaran de la mateixa manera i, en conseqüència, es redueix el marge per expressar-se lliurement.

Freqüentment s'argumenta que «no tenim res a amagar» i que, per tant, no ens ha de preocupar, però aquest argument és irrellevant pel que fa a la privacitat ja que aquesta no tracta d'amagar-se, sinó de mantenir l'autonomia, l'habilitat i la capacitat de poder decidir com presentar-se envers el món. Això contrasta amb el lema que domina el discurs públic: la transparència. Aquest imperatiu planteja qüestions interessants per analitzar ja que converteix en sospitosa qualsevol persona que no se sotmeti a la visibilitat. Des del punt de vista econòmic, el "bigdata" és una de les formes més lucratives d'operar serveis massius a internet que existeixen.

Aquest curs està dissenyat per exposar de forma amena quins són els riscos que impliquen les nostres activitats quotidianes i per desenvolupar habilitats per a preservar la nostra privacitat en

línia. El curs s'organitza a partir de presentacions teòriques i exercicis pràctics, dirigits a fomentar un ús conscient d'internet, xarxes socials i serveis web, alhora que es promou la conscienciació al voltant dels problemes socials i dels riscos que implica l'ús de tecnologies socials per a la seva privacitat i en alguns casos també la seguretat. S'explicarà com generem rastres digitals, alguns banals, com preferències sobre productes, i altres més personals, com la geolocalització o les preocupacions sobre la salut. Totes aquestes dades són recollides constantment sense que ens adonem i aquesta erosió sobre la privacitat pot tenir conseqüències a llarg termini en termes laborals, personals o econòmics entre d'altres.

Moltes persones senten que no es pot fer pràcticament res per evitar-ho i s'estén una sensació d'impotència que se sosté sobre la manca de coneixement i habilitats, que fa que es tendeixi a acceptar l'estat de vigilància com una cosa «natural» que s'ha d'acceptar; per això, resulta fonamental saber avaluar quins són els riscos als quals estem exposats i desenvolupar habilitats per a protegir-se dels mateixos quan es consideri necessari. És evident que no totes les persones tenen la mateixa percepció d'aquestes amenaces, tampoc totes es troben sota les mateixes circumstàncies. Els riscos que implica publicar una informació comprometedora no són els mateixos per a un periodista a Espanya que per a un altre col·lega a Hondures o a Moçambic. Els professionals de la informació poden beneficiar-se de les eines i d'una sèrie de senzilles pràctiques per establir comunicacions segures amb les seves fonts i preservar el seu anonimat i seguretat. Així, el dret de publicar informacions comprometedores pot complementar-se amb el nivell de seguretat que exigeix el discurs anònim; aquest és, cada vegada més, un requisit per exercir la llibertat d'expressió, perquè no es pot tenir discurs anònim si no es té una forta protecció de la privacitat.

## 2. Justificació

Els motius per crear aquest curs d'especialització es fonamenten en la preocupació per sensibilitzar la societat i els professionals de la informació sobre la necessitat de defensar i millorar drets fonamentals

A partir dels continguts que s'aborden en el curs es vol incidir en com mantenir, reconstruir o reinventar formes de comunicar-se amb confiança i seguretat. Es tracta, per tant, d'una aproximació política a les tecnologies de la informació i la comunicació a partir de la qual es planteja la necessitat d'entendre com funciona el codi del qual depenen les seves vides en l'actualitat, ja que no fer-se aquesta pregunta és com signar un contracte sense saber llegir. El curs no està plantejat per experts en seguretat o informàtica, sinó que tracta de fer accessibles

una sèrie de tàctiques i habilitats per mostrar que no cal ser programador o especialista per tenir la capacitat d'actuar com a agents de canvi. El programari lliure, el maquinari lliure i els serveis web descentralitzats són excel·lents alternatives als béns i serveis comercials, ja que inclouen una visió de la tecnologia que es construeix a partir d'uns principis més justos, basats en la cooperació i que proposen usos tecnològics a partir dels quals es pot fer que la recopilació i agregació de dades sigui molt més difícil. D'aquesta manera, permet que totes les persones involucrades en el seu ús formin part i siguin agents actius en el control d'una porció de la infraestructura sobre la qual es du a terme la comunicació i, d'aquesta manera, desenvolupin hàbits més segurs a l'hora de connectar-te a la xarxa.

En definitiva, es tracta d'aportar coneixements i habilitats per al desenvolupament de la sobirania tecnològica en el camp de la comunicació. El contingut es presenta de manera que sigui fàcil la seva assimilació, sense aprofundir en complexos assumptes tècnics sobre privacitat i anonimat, però sí fent-ho sobre conceptes que són abstractes per a molta gent. D'aquesta manera es pretén que els participants desenvolupin una consciència crítica que els permeti discernir que la vigilància massiva no tracta tant de la privacitat, sinó del nostre dret a la intimitat. Així com les implicacions i el cost de l'ús de serveis «gratuïts».

### 3. Resultats esperats del programa

#### 3.1. OBJECTIUS FORMATIUS

- ~ Exposar i debatre sobre les implicacions de la pèrdua de privacitat en les comunicacions per visibilitzar i sensibilitzar sobre les seves conseqüències
- ~ Conèixer les eines i recursos disponibles per preservar la privacitat
- ~ Adquirir i desenvolupar habilitats per desenvolupar hàbits segurs en la xarxa

#### 3.2. COMPETENCIES ESPECÍFIQUES

- ~ Avaluació de risc en la comunicació
- ~ Gestió de rastres digitals
- ~ Ús bàsic de GNU / Linux i eines per millorar la seguretat i privacitat
- ~ Desenvolupar habilitats per enfortir la privacitat i protecció de periodistes i les seves fonts

#### 3.3. SALIDAS PROFESIONALES

- ~ Comunicació

- ∨ Periodisme
- ∨ Docència

## 4. Pla D'Estudis

### 4.1. CONTINGUTS

Al llarg del curs es presentarà en cadascuna de les sessions una breu introducció teòrica que es complementarà amb una sèrie d'exercicis pràctics sobre cadascun dels temes abordats. Els continguts tracten de donar una base teòrica, a partir de la qual s'estableix un estat de la qüestió, i de desenvolupar habilitats i pràctiques segures al voltant de la gestió de dades personals i usos de serveis basats en internet.

### 4.2. MÓDULS

Assgnature	Descripció de continguts de l'assignatura
1. La privacitat i seguretat en la societat de la transparència	Presentació del curs. Taula rodona i debat 1. Què és privacitat, transparència, i seguretat. implicacions per a la democràcia 2. Actors: estat i empreses 3. Comunicació i periodisme preservació de l'anonimat de fonts 4. Participació política i esfera pública a la xarxa
2. Intro a GNU/Linux	1. Sistemes Operatius lliures, Instal·lació i usb-live 2. Escriptoris 3. Software i gestió de paquets 4. Consola i línia d'ordres
3. DADES PERSONALS	1. Què són i per què haurien d'importar? 2. Avaluació de riscos 3. Gestió de claus Keepassx 4. Navegació segura i privada. Plugins per privacitat / seg. 5. Cercadors alternatius 6. Tor i Tails 7. Publicació i difusió, bústies anònims 8. Xarxes socials federades

4. Comunicacions xifrades	<ol style="list-style-type: none"> <li>1. Mail, xat i videoconferència</li> <li>2. Correus temporals</li> <li>3. Gestió de claus</li> </ol>
5. PROTECCIÓ	<ol style="list-style-type: none"> <li>1. Recuperació de dades (photorec i distribucions tipus Knopixx) Truecrypt / Ciphershed</li> <li>2. Esborrat de l'espai buit i configuració de la paperera per a l'eliminació integral d'arxius (mac): Ccleaner / BleachBit (win / linux)</li> <li>3. Metadata (foto i vídeo) exif tools (mac), shred (linux)</li> <li>4. Xifrat: Truecrypt / Ciphershed</li> </ol>
6. Telèfons mòbils	ROMS / APPS per a navegació segura i comunicació xifrada

## 5. Professorat

- **Núria Saura** - Doctora en dret i professora de Llibertat d'expressió (UAB - Facultat de Ciències de la Comunicació)
- **Xosé Quiroga** - Tècnic Superior en fotografia (Escola d'Arts Pablo Picasso, la Corunya). Llic. En Dret (univ. La Corunya). Membre fundador del Voizes Archive, el col·lectiu Groundpress i del projecte formatiu Ago didàctica
- **Simón Vialás** - Doctor en comunicació. Investigador (InCom-UAB), docent i productor audiovisual

## 6. Perfil dels estudiants

El curs està adreçat a qualsevol persona que tingui inquietud per desenvolupar pràctiques comunicatives segures i en relació amb l'accés a informació. Particularment, es dirigeix a periodistes i professionals de la informació que vulguin desenvolupar habilitats per protegir les seves fonts i també per dotar-los de coneixements per poder crear bústies anònims per rebre filtracions de manera anònima. També per a educadors que vulguin incorporar aquest tipus de coneixements en els seus plans d'estudi

### 6.1. REQUISITOS DE ACCESO



# Formació

- ∨ No cal tenir coneixements previs sobre programari lliure
- ∨ Ordinador persona