

Gloria González Fuster in Dariusz Kloza (ur.)

Evropski priročnik za poučevanje zasebnosti in varstva osebnih podatkov v šolah



EVROPSKI PRIROČNIK ZA POUČEVANJE
VARSTVA ZASEBNOSTI IN OSEBNIH PODATKOV V ŠOLAH

EVROPSKI PRIROČNIK
ZA POUČEVANJE
VARSTVA ZASEBNOSTI IN
OSEBNIH PODATKOV V ŠOLAH

Uredila

Gloria GONZÁLEZ FUSTER
Dariusz KLOZA

EAP

Evropski priročnik za poučevanje varstva zasebnosti in osebnih podatkov v šolah
© Gloria GONZÁLEZ FUSTER in Dariusz KŁOZA (ur.) 2016

To delo je nastalo v okviru projekta ARCADES (<http://www.arcades-project.eu/>), katerega tema je Vnašanje tematike varstva osebnih podatkov in zasebnosti v šole v Evropski uniji, in je potekal od novembra 2014 do maja 2016, sofinanciran s strani programa "Temeljne pravice in državljanstvo" pod okriljem Generalnega direktorata za pravosodje in potrošnike pri Evropski komisiji (številka pogodbe JUST/2013/FRAC/AG/6132).

Opozorilo: vsebina tega dela ne odseva nujno pogledov Evropske komisije.

Priročnik za učitelje in Mini listina pravice do zasebnosti in varstva osebnih podatkov sta izdana pod mednarodno licenco Creative Commons Attribution 4.0

ISBN 978-94-000-0770-3
D/2016/7849/113
NUR 822

Naslovna ilustracija: © Femke Vanhellemont, 2016
na podlagi fotografije: © Nina Jelen, 2016.

Ilustraciji na str. 98 in 99: © Anže Novak
Ilustracija na str. 83: © Tomasz Soczyński

O slovenski izdaji publikacije:

Prevedli (v abecednem vrstnem redu): Urban Brulc, Jelena Burnik, Matjaž Drev, Saša Zlatkovski, Vanja Zrimšek.

Pregledale in uredile: Jelena Burnik, Polona Tepina, Vanja Zrimšek.

ZAHVALE

Zahvala za delo, ki je pred vami, gre številnim učiteljem, strokovnjakom s področja izobraževanja, zasebnosti in varstva osebnih podatkov ter drugih področij, aktivistom s področja varovanja zasebnosti, oblikovalcem politik, otrokom in mladim, ki so nas med razvojem projekta ARCADES podpirali in spodbujali.

Še posebej smo hvaležni članom Mednarodne delovne skupine za varstvo osebnih podatkov in digitalno izobraževanje, s koordinatorko Pascale Serrier (*Commission Nationale de l' Informatique et des Libertes – CNIL*), poljskemu izobraževalnemu centru Gliwice – *Gliwicki Ośrodek Metodyczny*) in Kirsten Fiedler (*European Digital Rights – EDRI*) za njihove dragocene povratne informacije o priročniku za učitelje. Hvaležni smo *Autoritat Catalana de Proteccio de Dades* (APDCAT) in *Eticas Research & Consulting* za njihov neprecenljiv prispevek k zaključni konferenci ARCADES. Za pomoč na različnih stopnjah projekta bi se radi zahvalili tudi Evropskemu šolskemu omrežju (*European Schoolnet*), Aidi Barquero in Centru za IT izobraževanje in računalniške aplikacije v Varšavi (*Ośrodek Edukacji Informatycznej i Zastosowan Komputerow – OEIiZK*).

Ne nazadnje gre naša iskrena zahvala vsem učencem in učiteljem, ki so sodelovali na natečaju za najboljšo učno uro zasebnosti. Samo nekaj je bilo zmagovalcev, vendar so bili prav vsi navdihujoči.

Skupina ARCADES

VSEBINA

<i>Zahvale</i>	v
<i>Seznam uporabljenih kratic</i>	xiii

Predgovor: Zakaj ARCADES?

Wojciech RAFAŁ WIEWIÓROWSKI	1
-----------------------------------	---

Uvodni nagovori partnerjev projekta ARCADES	5
---	---

Raziskovalna skupina za pravo, znanost, tehnologijo in družbo (LSTS)	5
Glavni inšpektor za varstvo osebnih podatkov Poljske (GIODO)	7
Informacijski pooblaščenec Republike Slovenije (IP RS)	9
Madžarski Nadzorni organ za varstvo osebnih podatkov in prost dostop do informacij	11

I. DEL

PREGLED PODROČJA IZOBRAŽEVANJA O ZASEBNOSTI IN VARSTVU OSEBNIH PODATKOV

ARCADES, evropski projekt za spodbujanje izobraževanja o zasebnosti..... 15

1. Številne pobude na nacionalnih ravneh.....	15
2. Poljske izkušnje	16
3. Nujnost izobraževanja o zasebnosti in varstvu osebnih podatkov	16
4. Cilji projekta ARCADES – za kaj gre?	17
5. Doseganje ciljev	18
6. Evropska naravnost in obeti za prihodnost	20

Sporočilo Delovne skupine za digitalno izobraževanje

Pascale RAULIN-SERRIER in Sophie VULLIET-TAVERNIER	21
--	----

Številne podobe izobraževanja na področju zasebnosti v evropskih šolah

Gloria GONZÁLEZ FUSTER, Dariusz KLOZA in Paul DE HERT.....	23
--	----

1. Zakaj izobraževanje o zasebnosti?	23
1.1. Težave s posegi v zasebnost so resnične in pogosto z resnimi posledicami.....	23
1.2. Zakoni o varovanju zasebnosti ponujajo univerzalno zaščito in opolnomočenje posameznikov	25
1.3. Zakonodaja o varovanju zasebnosti prepoznava pomen posebnih varovalk za otroke.....	26
1.4. Nekaterim težavam na področju zasebnosti se lahko izognemo tako, da se jih zavedamo	27
1.5. Opolnomočenje najbolj ranljivih.....	28
2. Pregled stanja na področju izobraževanja o zasebnosti v Evropi.....	30
2.1. Kdo?.....	30
2.2. Kje in kdaj?	31
2.3. Kako?.....	31
2.4. Kaj?	34
3. Zaključne misli	36

II. DEL

PRIROČNIK ZA UČITELJE

Predstavitev priročnika za učitelje	41
1. O zasebnosti.....	42
Cilji	42
Ključni poudarki	42
Primeri iz resničnega življenja.....	43
Ideje za pogovor	43
Priporočene dejavnosti.....	44
Za najmlajše	44
Za starejše in/ali bolj zrele.....	44
2. O varstvu osebnih podatkov.....	45
Cilji	45
Ključni poudarki	45
Primeri iz resničnega življenja.....	47
Ideje za pogovor	47
Priporočene dejavnosti.....	47
Za najmlajše	48
Za starejše in/ali bolj zrele.....	48

3. Kdo želi tvoje osebne podatke?	49
Cilji	49
Ključni poudarki	49
Ideje za pogovor	50
Priporočene dejavnosti.....	51
Za najmlajše	52
Za starejše in/ali bolj zrele	52
4. Odloči se pametno in pusti drugim, da se odločijo sami	53
Cilji	53
Ključni poudarki	53
Ideje za pogovor	55
Priporočene dejavnosti.....	55
Za najmlajše	56
Za starejše in/ali bolj zrele	56
5. Spletna identiteta	57
Cilji	57
Ključni poudarki	57
Primeri iz resničnega življenja	58
Nasveti.....	59
Ideje za pogovor	60
Priporočene dejavnosti.....	60
Za najmlajše	61
Za starejše in/ali bolj zrele	61
6. Spletno oglaševanje.....	62
Cilji	62
Ključni poudarki	62
Ideje za pogovor	63
Priporočene dejavnosti.....	64
Za najmlajše	65
Za starejše in/ali bolj zrele	65
7. Kako ohraniti skrivnosti res skrite?.....	66
Cilji	66
Ključni poudarki	66
Nasveti.....	68
Priporočene dejavnosti.....	69
Za najmlajše	71
Za starejše in/ali bolj zrele	71
8. Družina, zasebnost in varstvo osebnih podatkov.....	72
Cilji	72

Ključni poudarki	72
Primeri iz resničnega življenja.....	73
Ideje za pogovor	73
Priporočene dejavnosti.....	74
Za najmlajše	74
Za starejše in/ali bolj zrele.....	75
9. Bodi varen in se dobro imej.....	76
Cilji	76
Ključni poudarki	76
Ideje za pogovor	77
Priporočene dejavnosti.....	78
Za najmlajše	79
Za starejše in/ali bolj zrele.....	79
10. Kako ukrepati?.....	80
Cilji	80
Ključni poudarki	80
Priporočene dejavnosti.....	82
Za najmlajše	82
Za starejše in/ali bolj zrele.....	82
Mini listina pravice do zasebnosti in varstva osebnih podatkov.....	83
Predstavitev izbranih učnih ur.....	87
1. Primer učne ure 1: Mali škratje	
Nina JELEN	89
1.1. Najboljše šolsko leto	89
1.2. Načrt učne ure.....	90
1.2.1. Opis	90
1.2.2. Potek učne ure	91
1.2.3. Učni pripomočki	94
1.2.3.1. Pesem	94
1.2.3.2. Izmišljeni obrazec za registracijo	97
1.2.3.3. Zlata pravila faconk in faconov na internetu.....	98

2. Načrt učne ure 2: Kdo želi vaše osebne podatke?	
Małgorzata SZYSZKO in Katarzyna WIĄCZEK	99
2.1. Uvod	99
2.2. Načrt učne ure	100
2.2.1. Opis	100
2.2.2. Potek učne ure	101
2.2.2.1. Uvod (osnovno znanje)	101
3. Načrt učne ure 3: Spletne nevarnosti	
Eszter KESZY-HARMATH	105
3.1. Prihodnost se je začela	105
3.2. Načrt učne ure	106
3.2.1. Opis	106
3.2.2. Potek učne ure	106
<i>Slovarček</i>	109
<i>Uporabni viri</i>	111

SEZNAM UPORABLJENIH KRATIC

ARCADES	Projekt vnašanja tematike varstva osebnih podatkov in zasebnosti v šole v Evropski uniji
CNIL	Commission Nationale de l'Informatique et des Libertés
EU	Evropska unija
GIODO	Generalny Inspektor Ochrony Danych Osobowych
IP RS	Informacijski pooblaščenec Republike Slovenije
IT	Informacijske tehnologije
LSTS	Research Group on Law, Science, Technology and Society
NAIH	Nemzeti Adatvédelmi és Információszabadság Hatóság
OEIiZK	Ośrodek Edukacji Informatycznej i Zastosowań Komputerów; Centre for IT Education and Computer Applications in Warsaw
VUB	Vrije Universiteit Brussel

PREDGOVOR

ZAKAJ ARCADES?

Wojciech RAFAŁ WIEWIÓROWSKI*

Tehnologija ima na današnjo družbo in ekonomski razvoj nedvomno ogromen vpliv. Nove generacije mladih se med informacijskimi tehnologijami (IT) počutijo bolj domače kot so se njihovi starši in stari starši. Del iste zgodbe je tudi naraščajoča uporaba mobilnih, »pametnih« naprav in aplikacij, ki omogočajo intenzivno zbiranje podatkov in precejšnje neravnovesje med ponudniki takih naprav in aplikacij na eni strani ter potrošniki na drugi. Tu so družbene koristi povezane s pomembnimi tveganji za posameznikovo pravico do zasebnosti in varstva osebnih podatkov, znanje o upravljanju z informacijami in digitalne spretnosti pa so temeljne zahteve za generacijo mladih. Glede na povedano je poslanstvo nadzornih organov za varstvo osebnih podatkov to, da mlade ustrezno pripravimo na izzive, medtem ko družba izkorišča pozitivne strani tehnologije.

Koncept projekta ARCADES temelji na Poljskem nacionalnem programu za šole iz leta 2009, poimenovanem »*Tvoji podatki - tvoja skrb*« in na relativno velikem interesu, ki so ga za ta program pokazali učitelji na Poljskem. To je bil navdih za poljski nadzorni organ za varstvo osebnih podatkov, da prenese idejo na evropsko raven. Projektna skupina je verjela, da bi šole morale poučevati učence tudi o zasebnosti in varstvu osebnih podatkov in da bi te teme lahko vključile v učne programe različnih šolskih predmetov. To je del digitalnih spretnosti, ki so temelj znanja v 21. stoletju in osnovni pogoj za razvoj sodobnega državljana. Poudarek je tudi na tem, da demokratična družba potrebuje mlade, ki bodo znali digitalne aktivnosti uporabljati v smislu spoštovanja človekovih pravic in kot orodje, s katerim bodo spreminjali svet. Digitalne spretnosti omogočajo

* Namestnik Evropskega nadzornika za varstvo osebnih podatkov

družbeno dejavnost in pomagajo pri razvoju podjetništva, umetnosti in inovacij. Mlad človek, ki želi uporabljati digitalne tehnologije praktično in učinkovito, pa se mora zavedati, da, medtem ko podatki predstavljajo gorivo nove ekonomije, uporabnik, ki se ne zaveda skrbi glede zasebnosti pri obdelavi osebnih podatkov, lahko postane le »produkt« v tej industrijski verigi.

Evropski organi za varstvo osebnih podatkov v svojem »Mnenju o varstvu osebnih podatkov otrok« (Mnenje 2/2009 Delovne skupine iz člena 29) poudarjajo, da oseba, ki še ni dosegla fizične in psihološke zrelosti, potrebuje več zaščite kot ostali. Izboljšanje pogojev in krepitev otrokovih pravic za razvoj njegove osebnosti pa ne pomenita le ukrepov zakonodajalca ali organov za varstvo podatkov. Najprej je treba delati na posredovanju znanja o zasebnosti pri uporabi novih tehnologij, in sicer prav v vsaki fazi otrokovega izobraževanja.

Varovanje otrok in skrb za njihovo dobro počutje se nanašata na otrokovo pravico do razvoja in na dejstvo, da je otroštvo mogoče uživati le ob pomoči in zaščiti s strani drugih. To zaščito prinašajo tako družina kot tudi družba in država. Treba se je zavedati, da ustrezna raven zaščite otrok hkrati pomeni tudi, da bodo morale različne institucije obširneje obdelovati njihove osebne podatke. Pristop k varovanju zasebnosti otrok mora temeljiti na izobraževanju (s pomočjo družine, šole, organov za varstvo osebnih podatkov, skupnosti otrok in drugih) o pomembnosti varstva osebnih podatkov in zasebnosti ter o posledicah razkrivanja osebnih podatkov, kadar to ni potrebno.

Če želimo kot družba stremeti k resnični kulturi varovanja osebnih podatkov in zasebnosti, moramo začeti pri otrocih. Ne le zato, ker so skupina, ki potrebuje zaščito in katerih pravice je treba varovati, temveč tudi zato, da bi se ti zavedali svojih dolžnosti spoštovanja varovanja osebnih podatkov drugih oseb. Ključno vlogo pri doseganju tega cilja pa imajo šole.

Otroci in učenci bi morali biti vzgojeni tako, da bi postali svobodni državljani informacijske družbe. Ključno je, da bi se morali že v zgodnjem otroštvu učiti o pomembnosti zasebnosti in varovanja osebnih podatkov. Tako bi lahko sprejemali informirane odločitve o tem, katere informacije želijo razkriti, komu in pod kakšnimi pogoji. Varovanje osebnih podatkov bi moralo biti sistematično vključeno v šolske učne programe, ne nujno kot poseben predmet, temveč z upoštevanjem šolskega razreda, starosti otrok in tudi narave poučevanih predmetov.

Razvoj digitalnih spretnosti običajno temelji na iskanju ravnovesja med zmožnostmi tehnologije in praktičnim rezultatom, ki ga je treba doseči. Izobraževalne dejavnosti za varovanje zasebnosti bi morale sloneti na »dobim – dobiš« scenariju. Morali pa bi se zavedati, da so zmožnosti glede digitalnih veščin odvisne tudi od lastnosti posameznika ter da se razlikujejo od otroka do otroka.

Javne in zasebne izobraževalne ustanove ter civilna družba, ki je vključena v izobraževalne procese, bi morale na vprašanja varovanja osebnih podatkov gledati kot na enega glavnih ciljev pridobivanja digitalnih veščin in spodbujati inovativne načine poučevanja zasebnosti ter otrokom zagotavljati praktična orodja, s katerimi bodo lahko varovali svojo zasebnost.

Bruselj, maj 2016

UVODNI NAGOVORI PARTNERJEV PROJEKTA ARCADES

Raziskovalna skupina za pravo, znanost, tehnologijo in družbo (LSTS)*

Dame in gospodje,

Raziskovalna skupina za pravo, znanost, tehnologijo in družbo (LSTS) Vrije Universiteit Brussel (VUB) je ponosna na projekt ARCADES, še posebej pa na objavo tega priročnika.

Glavni cilj projekta ARCADES je bil okrepiti prizadevanja evropskih nadzornih organov za varstvo osebnih podatkov za dvig zavesti o varovanju zasebnosti med otroci in mladimi preko izobraževanja v šolah. Da bi to dosegli, smo se v projektu povezali LSTS z VUB, vodilna raziskovalna skupina z mednarodno priznanim ugledom na področju varovanja zasebnosti in osebnih podatkov (in pomembnimi izkušnjami pri skupnem delu z organi za varstvo osebnih podatkov) in štirje organi za varstvo osebnih podatkov. Kot edini partner projekta ARCADES z akademskim ozadjem smo imeli nalogo, da usmerjamo konzorcij k dokončanju tega priročnika: praktičnega, inovativnega, izrazito evropskega in v prihodnost usmerjenega referenčnega besedila za učitelje.

Med projektom smo se veliko naučili. Vedeli smo, da so nadzorni organi za varstvo osebnih podatkov skušali doseči tako otroke in mlade kot tudi njihove učitelje. S pomočjo projekta ARCADES smo odkrili, da obstaja bogata bera pobud na to temo, da so organi tem ciljem predani in da učitelji ne potrebujejo le smernic s tega področja, pač pa so zelo zainteresirani za to, da jih delijo z učenci.

* Vrije Universiteit Brussel (VUB).

Vedno smo verjeli, da je otrokom in mladim mar za zasebnost in da jih ne smemo obtoževati, da se ji odrekajo, pač pa, da jih bolje poučimo, kako naj jo ubranijo. Projektu ARCADES gredo zahvale, da smo se spoznali z otroki in mladimi, ki so nas naučili, kako pomembno je imeti nadzor nad svojimi osebnimi podatki in da nihče ni premlad, da bi razmišljal o zasebnosti.

Od samega začetka smo imeli vizijo, da bomo pri delu na tem priročniku upoštevali vse dostopne materiale in pomembno znanje, ki je na voljo v Bruslju in širše. Vključili smo povratne informacije učiteljev in njihovih učencev pa tudi strokovnjakov s področja izobraževanja; upoštevali smo civilno družbo, strokovnjake za spletno varnost ter širšo skupnost nadzornih organov za varstvo osebnih podatkov.

Vsa naša prizadevanja so bila povezana z varovanjem zasebnosti in osebnih podatkov kot temeljnih pravic. Ne smemo namreč pozabiti, da sta obe pravici zaradi njune pomembnosti za demokratično življenje navedeni v Listini Evropske unije o temeljnih pravicah. Poučevanje o zasebnosti in varovanju osebnih podatkov zato ne sme poudarjati le tega, kako »zaščititi« mladoletnike, temveč jih je treba ozaveščati o temeljnih pravicah in njihovem uveljavljanju.

Nastanek tega priročnika je tako po našem mnenju enkratna novica, ne samo za učitelje, ampak tudi za vsakega, ki verjame, da izobraževanje lahko pomaga otrokom in mladim, da postanejo boljši (digitalni) državljani.

Prof. dr. Paul De Hert
Bruselj, maj 2016

Glavni inšpektor za varstvo osebnih podatkov Poljske (GIODO)

Dame in gospodje,

ponosni smo, da vam lahko predstavimo to publikacijo, ki je dokaz leto in pol trajajočega dela, namenjenega uvajanju tematike varovanja osebnih podatkov in zasebnosti v šole. Zelo sem zadovoljna, da sem bila lahko, kot glavna nadzornica za varstvo osebnih podatkov, del tega projekta.

V Evropski uniji je pripravljenega veliko izobraževalnega gradiva o varstvu osebnih podatkov v digitalnem svetu, ki je namenjeno otrokom, mladim in staršem. Glede na to, da otroci začnejo že v zgodnjem otroštvu uporabljati splet za učenje, zabavo in komunikacijo, njegova vrednost v dobi hitrega tehnološkega razvoja ne smemo podcenjevati. Na žalost pa otroci zelo pogosto nepremišljeno delijo informacije o sebi in drugih. Kljub temu da je na spletu dostopnega veliko izobraževalnega gradiva, je vloga šole v procesu izobraževanja nenadomestljiva.

Ko smo začeli delati na projektu ARCADES, smo si za cilj zastavili oblikovanje praktičnega gradiva za šole in učitelje, z namenom, da bi jim pomagali poučevati o pomembnosti varovanja zasebnosti na zanimiv in obenem učinkovit način. Prepričani smo, da bi morale znanje o varovanju zasebnosti in osebnih podatkov ter varni rabi interneta predstavljati enega bistvenih elementov šolskega izobraževanja. Ta publikacija ponuja praktične napotke za poučevanje o tej temi.

Rezultati natečaja za najboljšo učno uro iz zasebnosti, ki smo ga v sklopu projekta ARCADES izvedli za šole na Poljskem, nam kažejo tudi dejansko vrednost tega gradiva. Učitelje smo namreč povabili, da na podlagi praktičnega dela priročnika razvijejo model učne ure o varovanju osebnih zasebnosti. Prejeli smo ducat odličnih predlogov, ki so izpolnjevali tudi metodične zahteve, obvezne na Poljskem. Veliko prejetih del je pokazalo, kako na izviren in učinkovit način poučevati otroke in mlade o varovanju osebnih podatkov, pa tudi o temeljnih pravicah in njihovi pravilni uporabi.

Torej, več kot zadovoljni smo, da vam lahko predstavimo ta priročnik, v upanju, da bo dobro sprejet tako med učitelji v Evropski uniji in v celotni evropski izobraževalni skupnosti kot tudi pri vseh organih za varstvo podatkov v EU.

Dr. Edyta Bielak-Jomaa

Varšava, maj 2016

Informacijski pooblaščenec Republike Slovenije (IP RS)

Dame in gospodje,

v veliko zadovoljstvo mi je, da vam lahko predstavim to publikacijo, ki je plod odličnega sodelovanja med partnerji projekta ARCADES. V njej boste našli ključne informacije o varovanju osebnih podatkov in zasebnosti, ki bi se jih morali zavedati otroci v šolah, kot tudi praktična orodja, ki bodo v pomoč učiteljem pri poučevanju teh tematik.

Zakaj smo se lotili projekta? Vsak dan se, kot nadzorni organ za varstvo osebnih podatkov, soočamo z vprašanji, primeri in pritožbami, ki zadevajo otroke; včasih v vlogi žrtev, ker je bila kršena njihova zasebnost, lahko pa celo v vlogi storilcev, ki ustrahujejo druge otroke na internetu ali socialnih platformah. Zato menimo, da je izobraževanje otrok ključno – bolje je preprečiti kot zdraviti. Mlade je treba učiti, kako naj varujejo svoje osebne podatke in zasebnost in kako lahko uporabljajo nove tehnologije odgovorno in s skrbnostjo do drugih.

Informacijski pooblaščenec Republike Slovenije je zelo dejaven na področju ozaveščanja. Vsako leto izdamo gradiva, katerih cilj je varna in odgovorna uporaba novih tehnologij. Vemo tudi, kako pomembno vlogo igrajo starši, učitelji in strokovnjaki s področja izobraževanja pri usposabljanju otrok, da bi ti odgovorno uporabljali informacijske storitve, izkoristili njihove pozitivne plati in pri tem ostali varni. Otroci so lahko v tehničnem znanju o uporabi interneta pred odraslimi, vendar pa jim manjka izkušenj in zavedanja elementa časa. Pred seboj imajo še celo prihodnost in pogosto se ne zavedajo, da jih bodo nekega dne podatki, ki jih sedaj objavljajo na spletu, lahko preganjali. Zaradi tega morda ne bodo dobili štipendije, službe, ki jo bodo želeli, partnerja v katerega bodo zaljubljeni. To zavedanje in perspektivo jim lahko ponudimo odrasli.

Projekt ARCADES smo začeli pred letom in pol in v tem kratkem času dosegli pomembne cilje. Napisali smo priročnik za poučevanje o zasebnosti in varstvu osebnih podatkov, ki je namenjen vsem učiteljem v EU. Organizirali smo tudi zelo uspešna izobraževalna seminarja za učitelje in strokovnjake s področja

izobraževanja. Povratne informacije učiteljev v Sloveniji so bile zelo pozitivne; povedali so nam, da so na seminarjih dobili veliko dragocenega znanja v praktični obliki primerov in interaktivnih vsebin, ki jih bodo lahko uporabili v praksi v svojih razredih. Prav tako smo organizirali natečaj za najboljšo učno uro in na naše veliko zadovoljstvo so zmagali prav učenci iz najmlajše starostne skupine, ki so šele začeli obiskovati osnovno šolo in so tik pred odkrivanjem potencialov interneta.

Če povzamem, v projektu ARCADES so nastali številni oprijemljivi rezultati, ki bodo pripomogli h krepitvi zavesti o varstvu osebnih podatkov in zasebnosti med otroki v šolah. Moja velika želja je, da bi ta publikacija dosegla čim več šol v različnih članicah EU in tako dvignila stopnjo znanja o varstvu zasebnosti in osebnih podatkov.

Mojca Prelesnik

Ljubljana, maj 2016

Nadzorni organ za varstvo osebnih podatkov in prost dostop do informacij Madžarske (NAIH)

Internetna kultura v vseh vidikih življenja vpliva na navade mladih, na njihovo mišljenje in obnašanje. Ustvarjajo se nove besede, v uporabi so nove oblike komunikacije, dogodki po vsem svetu se jih dotaknejo v trenutku in globalno. Te spremembe so neizogibne, vendar ne obsodbe vredne. Na tem področju je treba poudariti pomen ozaveščenosti, previdnosti, kritičnega pristopa in analitičnega odnosa.

Madžarski Nadzorni organ za varstvo osebnih podatkov in prost dostop do informacij (NAIH) je pričel delovati 1. 1. 2012. Organ nadaljuje s pravno dejavnostjo nekdanjega Pooblaščenca za varstvo podatkov, ki je deloval med leti 1995 in 2011. Madžarski organ za varstvo osebnih podatkov prejema pritožbe državljanov in v primeru utemeljenega suma hudih kršitev varstva osebnih podatkov lahko sproži tudi upravne postopke.

Obseg osebnih podatkov in podatkov v javnem interesu, ki se obdelujejo na internetu, je ogromen, tako z vidika količine informacij kot tudi številnih aktivnosti obdelave osebnih podatkov, števila udeleženih posameznikov ter moči neomejene medijske pozornosti. Varovanje osebnih podatkov otrok je bilo za nas, ki se ukvarjamo z vprašanji varstva osebnih podatkov, vedno prioriteta. Zaradi njihove starosti in pomanjkanja življenjskih izkušenj so bolj ranljivi, posledice kršitev pa lahko močno vplivajo na njihovo osebnost in duševni razvoj. Zato posvečamo posebno pozornost obdelavi osebnih podatkov na internetu, kadar ta vpliva na mladoletnike. Pri tem imata preventiva in širjenje informacij izreden pomen, ključno pa je tudi odpravljanje kršitev in ozaveščanje posameznikov, na katere se nanašajo osebni podatki.

Prepričani smo, da je uvajanje izobraževalnih tečajev o varstvu osebnih podatkov in zagotavljanje pravočasnega in praktičnega znanja ter usposabljanja učiteljev danes neizogibno, zato, da lahko učencem pomagajo postati usposobljeni in zavedni uporabniki modernih internetnih tehnologij ter samozavestni digitalni državljani. Uspeh naših publikacij – vključno s tem priročnikom – kaže, da je

med madžarskimi strokovnjaki, ki se ukvarjajo z otroki (učitelji, specialisti za varstvo otrok, dobrodельne organizacije) velika potreba po izmenjavi dobrih praks in znanja.

Seminar ARCADES je bil organiziran za 200 registriranih udeležencev – učiteljev in strokovnjakov s področja izobraževanja, od 20. 10. do 22. 10. 2015 v Budimpešti na Nacionalni univerzi za javne storitve. Program seminarja je bil razdeljen na dva dela: na plenarno zasedanje, kjer smo predstavili projekt in priložnik, medtem ko so praktične delavnice ponudile možnost diskusije s strokovnjaki o določenih temah, kot so osebnostne motnje, emocionalni učinki uporabe interneta ali praktični nasveti. Večina učiteljev je bila obveščena o dogodku preko ravnateljev, ki so povezani z mrežo Izobraževalnega inštituta, medtem ko so drugi novico o seminarju lahko zasledili na posebni spletni strani projekta ARCADES, ki jo je vzpostavil NAIH. Glede na neposredne odzive udeležencev na dogodkih in mnenja iz ocenjevalnih listov so bili seminarji uspešni in zelo uporabni. Poleg tega se 15 vlog, ki smo jih prejeli v okviru natečaja za *Najboljšo učno uro o zasebnosti*, sistematično sklicuje na teme in ideje iz priložnika, kot tudi na informacije in znanje, ki smo ga želeli deliti z udeleženci seminarjev.

V marcu 2016 smo pričeli skupaj z Ministrstvom za izobraževanje in univerzami, odgovornimi za usposabljanje učiteljev, pripravljati programe usposabljanja za varovanje osebnih podatkov za bodoče učitelje, ki jim NAIH z veseljem ponuja tudi svojo mednarodno mrežo, izkušnje in bazo znanj.

Dr. Attila Peterfalvi
Budimpešta, maj 2016

I. DEL
PREGLED PODROČJA IZOBRAŽEVANJA
O ZASEBNOSTI IN VARSTVU OSEBNIH
PODATKOV

ARCADES, EVROPSKI PROJEKT ZA SPODBUJANJE IZOBRAŽEVANJA O ZASEBNOSTI

Urszula GÓRAL IN Paweł MAKOWSKI*

1. ŠTEVILNE POBUDE NA NACIONALNIH RAVNEH

Med sodelovanjem v mnogih projektih, nekaterih financiranih tudi s strani EU, se je izkazalo, da prenekateri organi, pristojni za varstvo osebnih podatkov izvajajo tudi izobraževalne aktivnosti. Mnoge od teh zanimivih dejavnosti, ki so bile razvite na nacionalni ravni, so se v EU izvajale neodvisno oziroma vzporedno, čeprav so si bile v bistvu zelo podobne. Med sodelovanjem z drugimi organi je GIODO, poljski nadzorni organ za varstvo osebnih podatkov, zaznal potrebo po usklajevanju tovrstnih pobud z razširjanjem dobrih praks ter z zagotavljanjem dostopa do znanja. Lahko bi rekli, da je mednarodno sodelovanje med nadzornimi organi vodilo k temu, da so mnoge države same pričele z izobraževalnimi aktivnostmi in pri tem vlagale čas in napor v oblikovanje primernih orodij za izobraževanje in tudi že dosegle zadovoljive rezultate na tem področju. Zato se je zdelo primerno podpreti sinergijo med temi vzporednimi aktivnostmi in ustvariti skupno rešitev, ki bi omogočala bolj učinkovito izvajanje izobraževalnih dejavnosti nadzornih organov.

Vsak nadzorni organ se v svoji državi nedvomno sooča s podobnimi problemi in izzivi, kadarkoli načrtuje izvajanje izobraževalnih aktivnosti prek sodelovanja s šolami. Priprava primernih učnih pripomočkov, ustvarjanje privlačnih orodij za učitelje in učence ali usposabljanje učiteljev zahtevajo obsežne vire v smislu znanja in financiranja. Potrebno je tudi sodelovanje z organi, ki so pristojni za nadzor nad delovanjem šolstva. Kot kažejo izkušnje, je sodelovanje s temi organi

* Inšpektorat za varstvo osebnih podatkov (GIODO), Poljska.

(na primer na področju uvajanja vsebin, ki se nanašajo na varstvo osebnih podatkov in na pravico do zasebnosti v učne načrte) običajno uspešno. Z analizo teh aktivnosti je mogoče priti do določenega vzorca, ki bi ga lahko uporabili vsi nadzorni organi za varstvo osebnih podatkov, ki so zainteresirani izvajati tovrstne izobraževalne aktivnosti. Iz čezmejnega značaja interneta pa izhaja potreba po razvoju skupnega ter učinkovitega pristopa k poučevanju na evropski ravni.

2. POLJSKE IZKUŠNJE

V preteklih letih je GIODO v okviru svojih nalog poudarjal izobraževanje otrok in mladine preko številnih pobud oziroma aktivnosti. Čeprav se je soočal z običajnimi finančnimi težavami, je razvil zadovoljive rešitve, seveda s pomočjo drugih nadzornih organov in s povzemanjem njihovih izkušenj. Ena od takih dobrih izkušenj so aktivnosti češkega nadzornega organa. S tesnim sodelovanjem se je GIODO seznanil z njihovim pristopom k vpeljevanju vsebin, ki se nanašajo na zasebnost in osebne podatke v učne predmete, kot so literatura, biologija in zgodovina. Na podoben način je bil nato v šolah na Poljskem uspešno izveden program "*Tvoji podatki – tvoja skrb*". Glavni cilj tega programa, ki ga je GIODO neprekinjeno in uspešno izvajal šest let, je bil razširiti izobraževalno ponudbo poljskih Izobraževalnih centrov za učitelje, osnovnih in srednjih šol z vključevanjem vsebin, ki se nanašajo na osebne podatke in na pravico do zasebnosti. Ena od faz programa je bila usposobiti in opremiti učitelje, ki poučujejo v šolah in v Izobraževalnih centrih za učitelje z izobraževalnimi gradivi, ki vsebujejo informacije o varstvu osebnih podatkov kot tudi lekcije (učne ure ali učne scenarije) in tako dajo podlago učiteljem, da pri učencih oblikujejo zavedanje, odgovornost in odprtost. Drug element programa v šolah in izobraževalnih centrih za učitelje je bila izvedba učnih ur, ki se nanašajo na varstvo osebnih podatkov (poleg drugih vsebin), in tudi priprava osnutkov učnih scenarijev ter priprava ocenjevalnih poročil o aktivnostih, ki so bile izvedene v okviru programa.

3. NUJNOST IZOBRAŽEVANJA O ZASEBNOSTI IN VARSTVU OSEBNIH PODATKOV

Dosedanje izkušnje, ki so vplivale na politike na področju izobraževanja in oblikovanja sedanjih pristopov k izobraževanju in velik interes učiteljev na Poljskem za program "*Tvoji podatki – tvoja skrb*" so navdahnili GIODO za razširitev teh aktivnosti na evropsko raven. Rezultat tega je bil predlog projekta

ARCADES, marca 2014 poslan Evropski komisiji, v okviru programa “*Temeljne pravice in državljani*”, pod okriljem Generalnega direktorata za pravosodje in potrošnike. Predlog projekta je bil dokončno sprejet v juliju 2014 in na tej podlagi so bila zagotovljena sredstva za delo štirih projektnih partnerjev – poljskega Inšpektorata za varstvo osebnih podatkov (GIODO), slovenskega Informacijskega pooblaščenca (IP RS), madžarskega Nacionalnega organa za varstvo podatkov in prost dostop do informacij (NAIH) ter Raziskovalne skupine za pravo, znanost, tehnologijo in družbo pri Univerzi Vrije v Bruslju. Projektni konzorcij je bil sestavljen na podlagi izkušenj, ki so jih partnerji imeli na področju izvajanja in razvoja učnih pomoči v šolah.

4. CILJI PROJEKTA ARCADES – ZA KAJ GRE?

Projekt gre z roko v roki z drugimi evropskimi projekti, ki so namenjeni dvigu ozaveščanja o varstvu osebnih podatkov in zasebnosti. Kot že omenjeno, nadzorni organi v EU izvajajo mnoge podobne aktivnosti, ki neodvisno od njihovih siceršnjih pristojnosti namenjajo pozornost tudi izobraževanju. Varstvo osebnih podatkov in zasebnost sta temeljni pravici, ki ju varuje nacionalna in evropska zakonodaja. Naloga nadzornih organov je varovanje teh pravic, pa tudi širjenje znanja na tem področju. “*Resolucija o digitalni izobrazbi za vse*,” ki je bila pripravljena na Mednarodni konferenci pooblaščenecv za zasebnost in varstvo osebnih podatkov v Varšavi leta 2013, je primer take iniciative. Resolucija, ki priporoča, da bi morali biti mladoletni otroci deležni posebnega varstva zlasti na področju digitalnih tehnologij, je bila spodbuda za nadzorne organe, da se posvetijo tudi dejavnostim, ki bodo usmerjene v šolstvo.

To je izredno pomembno v času hitrega razvoja digitalnih tehnologij, katerih uporaba med mladimi je v porastu. Zato nadzorni organi pripravljajo izobraževalna gradiva, namenjena mladim, učiteljem in tudi staršem, saj je treba o varstvu osebnih podatkov in zasebnosti izobraževati tudi njih.

Tak način razmišljanja evropskih nadzornih organov podpira tudi nova Splošna uredba o varstvu osebnih podatkov, z dne 27. aprila 2016. Skladno s 57. členom je med drugimi nalogami nadzornih organov za varstvo osebnih podatkov predvidena tudi obveznost “*ozaveščanja in poučevanja javnosti o tveganju, pravilih, zaščitnih ukrepih in pravicah pri obdelavi osebnih podatkov*”. Zelo pomembno je, da omenjena določba poudarja potrebo po posvečanju posebne pozornosti otrokom.

Poljska izkušnja iz programa "Tvoji podatki - tvoja skrb" je pokazala, da je za razširjanje znanja o varovanju zasebnosti med otroki zelo pomembno uvesti te teme v učne ure oziroma v šolsko snov. Izkušnje z delom z učitelji, ki so sodelovali v programu, kažejo, da je pomembno pripraviti gradivo za učitelje zato, da lahko v šolah učinkovito in na privlačen način poučujejo snov s področja varstva osebnih podatkov. Posebna vloga šol pri izobraževanju otrok in mladine o delovanju družbe kot tudi za varno odkrivanje digitalnega sveta, je bila omenjena tudi v poročilu Eurobarometra za leto 2008 (*Za varnejšo uporabo interneta za otroke v EU – starševski vidik*). Prav v šolah otroci in mladina pogosto povedo o dogodkih, ki se nanašajo na kršitve zasebnosti. Glavni namen projekta ARCADES je bil zato pripraviti gradivo, ki bo v pomoč pri vpeljevanju tematik s področja varstva osebnih podatkov v šole v EU.

5. DOSEGANJE CILJEV

Pomemben pogoj za to, da bi učitelji lahko uspešno prenašali znanje s področja varstva osebnih podatkov, dvigovali zavest ter izboljšali veščine otrok in mladine na področju varstva zasebnosti, je primerno učno gradivo. Zato smo partnerji v projektu ARCADES najprej opravili raziskavo oziroma združili obstoječe znanje na področju poučevanja o varstvu zasebnosti in osebnih podatkov v šolah znotraj EU.¹ Rezultat je poročilo s pregledom informacij, gradivom o pravilih varstva zasebnosti in osebnih podatkov, namenjenim učiteljem in učencem ter dokumenti o glavnih trendih in običajnih (tudi najboljših) praksah. Dokument seveda ni izčrpen, zlasti glede na množico vseh izobraževalnih aktivnosti v EU, predstavlja pa vabilo k odprtju razprave o zahtevah, ki bi jim moralo učno gradivo slediti.

Na tej podlagi smo začeli s pripravo učnega gradiva, ki bi spodbudilo učitelje k poučevanju o varstvu osebnih podatkov in tako je nastal priročnik za učitelje.² Namenjen je učiteljem na osnovnih in srednjih šolah, ki bi želeli izboljšati znanje učencev na področju varstva osebnih podatkov, in sicer kot praktično gradivo, ki bo v pomoč pri izvajanju učnih vsebin, namenjenih tej temi. Cilj priročnika je postati uporabno orodje za učitelje v kateri koli šoli znotraj EU, ki bi želela

¹G. GONZÁLEZ FUSTER, P. DE HERT, AND D. KLOZA, Deliverable 1.1: State-of-the-Art Report on Teaching Privacy and Personal Data Protection at Schools in the European Union, ARCADES, marec 2015 <http://arcades-project.eu/images/pdf/State_of_the_art_report.pdf>dostop 01.05.2016.

²Za starejšo verzijo v slovenskem jeziku glej: G. González Fuster (ed.), Deliverable 1.2: *Evropski priročnik za učenje zasebnosti in varstva osebnih podatkov v šolah – gradivo za učitelje*, ARCADES, september 2015, https://www.ip-rs.si/fileadmin/user_upload/Pdf/arcades/ARCADES_prirocnik.pdf.

izobraževati otroke in najstnike o varstvu zasebnosti in osebnih podatkov. Napisan je v jasnem in preprostem jeziku, ki bo učiteljem v pomoč pri iskanju pravih besed pri razlagi najpomembnejših tem. Vsako od desetih tematskih poglavij učbenika pokriva eno od področij varstva zasebnosti in osebnih podatkov, ponuja vrsto ključnih idej in tem za razpravo ter vsebuje priporočene aktivnosti in konkretne nasvete. Prvi osnutek priročnika, katerega prenovljena verzija je predstavljena v tem gradivu, je bil deležen ugodnega odziva nacionalnih izobraževalnih institucij na Poljskem, Madžarskem in v Sloveniji, kar zagotavlja, da sledi zahtevam, ki veljajo za priročnike, ki se uporabljajo v šolah.

Priročnik je bil predstavljen na seminarjih, organiziranih v okvirju projekta ARCADES v oktobru 2015 s strani projektnih partnerjev iz Poljske, Madžarske in Slovenije. Vsakega od teh dogodkov se je udeležilo skoraj 200 učiteljev. Namen seminarjev je bil prenesti znanje o varstvu osebnih podatkov in zasebnosti zato, da bi ga učitelji prenašali dalje na svoje učence. Udeležencem dogodkov na Poljskem, Madžarskem in v Sloveniji so bile podane osnovne informacije o temah varstva osebnih podatkov in zasebnosti ter o priročniku. Odziv učiteljev kaže, da se pogosto srečujejo s tem, da nimajo dovolj znanja in virov, da bi otroke poučili o varstvu osebnih podatkov in zasebnosti. Poročali so tudi, da imajo v šolah pogosto incidente s področja kršitev varstva osebnih podatkov in zasebnosti, vendar nimajo na voljo dovolj navodil in usmeritev o tem, kako ukrepati. Zato smo v fazi ocenjevanja učinka z velikim zadovoljstvom pozdravili njihova pozitivna mnenja – dokazali so, da je bil vsak seminar uspešen in uporaben, kar utrjuje naše prepričanje, da v gradivu učitelji vidijo praktično vrednost.

To je bilo potrjeno tudi s številom prijav na tekmovanje za najboljšo učno uro, ki je bilo organizirano na Poljskem, Madžarskem in v Sloveniji. Izdajanje izobraževalnega gradiva in poučevanje zgolj na podlagi učbenikov pogosto ne prinaša želenih učinkov: nove metode poučevanja, ki sledijo potrebam učencev, bi morale biti uvedene v učne načrte zato, da bi se razvil učinkovit izobraževalni pristop. Izvajanje individualiziranega in življenjskega poučevanja lahko privabi pozornost in spodbudi otroško sodelovanje – poleg tega se ti naučijo, kako ukrepati v vsakodnevnih situacijah. Zato je bila tema natečaja priprava standardne učne ure, ki bi bila posvečena varstvu osebnih podatkov. Vsi scenariji, ki so bili pripravljene za natečaj, so bili zasnovani na osnovi gradiva iz projekta ARCADES, kar potrjuje njegovo uporabnost.

Zmagovalci nacionalnih natečajev za najboljšo učno uro so imeli priložnost predstaviti svojo učno uro na zaključni konferenci, ki je potekala marca 2015 v Barceloni. Hkrati je potekala tudi delavnica Mednarodne delovne skupine za varstvo osebnih podatkov in digitalno izobraževanje, ki jo koordinira francoski nadzorni organ za varstvo osebnih podatkov (CNIL). Delovna skupina je opazila aktivnost partnerjev projekta ARCADES, kar je vodilo v organizacijo skupnega dogodka v Barceloni, kjer smo obravnavali tovrstni model poučevanja in smernice za pridobitev “kompetenčnega okvirja” na področju varstva osebnih podatkov in zasebnosti.

6. EVROPSKA NARAVNANOST IN OBETI ZA PRIHODNOST

Do sedaj je bila večina dostopnega izobraževalnega gradiva s področja varstva zasebnosti in osebnih podatkov za otroke in mladostnike pripravljena na nacionalni ravni. Izmenjava izkušenj med partnerji projekta ARCADES je pomagala zasnovati ne samo učinkovito, temveč tudi bolj evropsko usmerjeno gradivo. To zlasti pomeni, da je partnerjem projekta uspelo pripraviti priročnik, ki ni specifičen za vsako državo, temveč je potencialno uporaben v katerikoli državi članici EU – čeprav je neizogibno potrebno nekaj prilagodljivosti za to, da bo praktično in neposredno uporaben v vsakem lokalnem okolju. Gradivo, ki je bilo zasnovano v tem projektu, zato predstavlja širšo perspektivo od zgolj nacionalne, kar ga dela prenosljivega in pripravljenega za uporabo v šolah po vsej EU.

Kljub temu da smo projekt pripeljali do konca, verjamemo, da bo ARCADES gradivo ostalo vir navdiha za mnoge učitelje v različnih državah članicah EU. Upamo, da bo to gradivo neposredno uporabno tudi za evropske nadzorne organe in za njihove izobraževalne aktivnosti, saj vsebina ne prinaša le nujnega znanja na področju poučevanja o zasebnosti, temveč tudi mnogo praktičnih nasvetov. Zato vabimo vse, da si pozorno preberejo to publikacijo in jo aktivno uporabijo ter na ta način prispevajo k spodbujanju izobraževanja o zasebnosti v Evropi.

SPOROČILO DELOVNE SKUPINE ZA DIGITALNO IZOBRAŽEVANJE

Pascale RAULIN-SERRIER in Sophie VULLIET-TAVERNIER*

*Resolucija o digitalni izobrazbi za vse,*¹ ki je bila sprejeta na 35. Mednarodni konferenci pooblaščenecv za zasebnost in varstvo osebnih podatkov v Varšavi leta 2013, je pozvala pristojne organe, da okrepijo svoje delovanje na področju izobraževanja, usmerjenega k celotni javnosti, da bi državljani postali informirani in odgovorni subjekti v digitalnem okolju, da bi učinkovito uporabljali svoje pravice in se zavedali tudi svojih dolžnosti na tem področju. V zadnjih letih so nadzorni organi iz različnih regij izmenjevali izkušnje in začenjali mnoge pobude za ozaveščanje otrok, mladine in izobraževalnih organizacij o varstvu osebnih podatkov in zasebnosti.

Omenjena resolucija je Mednarodni delovni skupini za varstvo osebnih podatkov in digitalno izobraževanje naložila uresničitev prednostnih aktivnosti, kot sta npr. *“Razvoj učnega paketa, ki je namenjen usposabljanju učiteljev na področju varstva osebnih podatkov in zasebnosti”* in *“Razvoj spletne platforme za izmenjavo vsebin in gradiv za poučevanje na področju digitalnega opismenjevanja”*.²

Evropski projekt ARCADES in priprava izobraževalnega gradiva pod njegovim okriljem se dobro povezuje z dejavnostmi priprave izobraževalnih paketov za usposabljanje učiteljev na področju varstva osebnih podatkov in zasebnosti.

* Oddelek za digitalno izobraževanje pri francoskem Nadzornem organu za varstvo osebnih podatkov - *Commission Nationale de l'Informatique et des Libertés* (CNIL), in koordinatorji Mednarodne delovne skupine za varstvo osebnih podatkov in digitalno izobraževanje.

¹<<https://icdppc.org/wp-content/uploads/2015/02/Digital-education-resolution.pdf>> dostopno 15. 05. 2016.

² To je: (1) Promocija izobraževanja o zasebnosti kot del programov za digitalno pismenost in (2) sodelovanje pri izvajanju izobraževanja v smislu “usposabljanja tistih, ki usposablajo” na področju varstva osebnih podatkov in zasebnosti.

Kakor kažejo analize³ za usposabljanje učiteljev za poučevanje varstva zasebnosti in osebnih podatkov v šolah znotraj EU ni na voljo poenotenih izobraževalnih pristopov, ki bi temeljili na evropski zakonodaji in hkrati zaobjeli posebnosti različnih evropskih pristopov.

Priročnik pred vami je namenjen učiteljem, da bodo lahko otrokom in mladostnikom pomagali razviti vse potrebne spretnosti, znanje in razumevanje, in se bodo ti lahko ustrezno in učinkovito odzvali na številne izzive in priložnosti vsakdanjega življenja v demokratični družbi, tako v fizičnem kot tudi v digitalnem svetu.

V tem kontekstu je namen priročnika in še posebej njegovega kompleta učnih pripomočkov preseči “medijsko pismenost” in “digitalno pismenost” in zaobjeti novi razsežnosti “pravne in etične pismenosti”, torej razumevanja, kje in kako relevantni predpisi določajo pravila obnašanja v *on-line* in *off-line* okolju.

Člani Mednarodne skupine za digitalno izobraževanje so pokazali veliko zanimanje za širjenje priročnika kot zelo koristnega in celovitega orodja, ki omogoča otrokom in najstnikom v celoti pridobiti znanje o svojih pravicah, svoboščinah in dolžnostih v demokratični družbi.

Učitelje spodbujamo, da gradivo preučijo in ga uporabijo ali priredijo ter raziščejo vsa področja v različnih poglavjih in jih uporabijo v skladu s svojimi pedagoškimi aktivnostmi in potrebami učencev. Ob koncu poudarjamo, da cenimo konzorcij projekta ARCADES in sodelujoče partnerje, ki so prispevali k nastanku tega inovativnega gradiva, in ga bodo razširjali med učitelji, mladimi in njihovimi starši.

³ Kot je prikazano v dveh poročilih Mednarodne delovne skupine za varstvo osebnih podatkov in digitalno izobraževanje, ki sta bili pripravljena v letu 2014 in 2015.

ŠTEVILNE PODOBE IZOBRAŽEVANJA NA PODROČJU ZASEBNOSTI V EVROPSKIH ŠOLAH

Gloria GONZÁLEZ FUSTER, Dariusz KLOZA in Paul DE HERT*

Izobraževanje na področju zasebnosti se v nekaterih evropskih šolah že odvija in marsikje se ta trend krepi. V tem prispevku raziskujemo, zakaj je tako in česa se lahko naučimo iz pregleda obstoječih praks. Na začetku so preučeni razlogi za poučevanje o zasebnosti v šolah, kasneje pa sledi pregled in ocena dosedanjih prizadevanj na tem področju. V zaključku ugotavljamo, da morajo biti otroci poučeni o varovanju zasebnosti, ne le, da bi bili varni, temveč, da jim to pomaga odrasti v svobodne posameznike.

1. ZAKAJ IZOBRAŽEVANJE O ZASEBNOSTI?

1.1. TEŽAVE S POSEGI V ZASEBNOST SO RESNIČNE IN POGOSTO Z RESNIMI POSLEDICAMI

Težave s posegi v zasebnost so resnične. Nekaterim, kot npr. avtorjem tega prispevka, ki se z vprašanji zasebnosti ukvarjamo dnevno, se to zdi skoraj samoumevno. Drugim pa nujnost in pomembnost vprašanj o zasebnosti ni tako očitna.

Začnimo z najbolj preprostim primerom. Mnogim ne bi bilo prijetno, če bi bila njihova imena, naslovi in poklici objavljeni na spletni strani župnije in to brez njihove privolitve. Podobno mnogi ne bi bili zadovoljni, če bi bile na taki spletni strani objavljene podrobnosti njihovega zdravstvenega stanja. Težava ni le v tem, da bi bile te informacije dostopne javnosti, temveč tudi, da bi lahko na njihovi podlagi sklepali tudi o drugih življenjskih okoliščinah nekoga, kot na primer, o

* Vrije Universiteit Brussel (VUB), Raziskovalna skupina za pravo, znanost, tehnologije in družbo (LSTS).

njegovi pripadnosti določeni verski skupnosti. Ta primer poudarja problematiko, ki jo je Sodišče Evropske unije obravnavalo že leta 2003 v zvezi s Švedinjo, gospo Bodil Lindquist, ki je na svoji spletni strani objavljala informacije o drugih brez njihove privolitve. Sodišče je odločilo, da je s tem kršila švedski zakon o varovanju osebnih podatkov.¹

Seveda obstajajo še drugi primeri neljubih dogodkov. Mnogi na svetu igrajo igrice na spletu in si tam ustvarjajo profile. Igranje pa je mogoče šele po registraciji, kjer mora posameznik razkriti nekaj osebnih podatkov in običajno plačati naročnino. *Sony PlayStation Network*, ena od takih storitev, je leta 2011 utrpela hekerski napad in osebni podatki približno 77 milijonov strank so bili javno razkriti. Ti podatki niso vsebovali le imen in elektronskih naslovov, temveč tudi uporabniška imena in gesla, rojstne podatke in podrobnosti o kreditnih karticah. Če bi to zadevalo le elektronske naslove, bi ljudje verjetno še dopustili nekaj neželenih elektronskih sporočil na teden. Informacije, kot so gesla in številke kreditnih kartic pa lahko povzročijo resnejše težave, tudi zato, ker večina ljudi uporablja isto geslo za več spletnih dejavnosti. *Sony* je nemudoma pozval svoje uporabnike, da naj bodo pozorni na porabo na svojih kreditnih karticah². Vendar pa to ni edini primer, incidenti v zvezi z osebnimi podatki se dogajajo dnevno, po vsem svetu³.

Pri takih kršitvah varstva osebnih podatkov in posegih v zasebnost se odpirajo vprašanja odgovornosti vpletenih. Včasih je odgovornost na posamezniku, ki se lahko odloči, katere podatke bo delil, ali bo, na primer, objavil informacije o drugih na spletu ali ne. Spet drugič pa ima ta lahko le majhno možnost vpliva, na primer, če je prisiljen v to, da sprejme določene prakse ravnanja s podatki zato, da lahko igra igro, ki jo je ravnokar kupil. V vseh primerih je mogoče, da se posamezniki ne zavedajo popolnoma posledic svojih odločitev, oziroma, kakšna so tveganja pri razkritju nekaterih osebnih podatkov.

Vse navedeno lahko razumemo kot problematiko zasebnosti, ki sega tudi na področje varstva osebnih podatkov in se pogosto prekriva z vprašanji tajnosti, varnosti in zavarovanja. Čeprav poseg v zasebnost ni edini zorni kot obravnave takih vprašanj, to ne spremeni dejstva, da ima poseg v zasebnost za posameznike

¹ Primer C-101/01, *Bodil Lindquist* (2003) ECR I-12971.

² PlayStation. Blog. Update on PlayStation Network and Qriocity, 26. 4. 2011
<http://blog.us.playstation.com/2011/04/26/update-on-playstation-network-and-qriocity>, dostopno 25. 5. 2016.

³ Za zanimivo vizualno predstavitev glej:
<<http://informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks>>, dostopno 20. 5. 2016.

lahko resne posledice. Posegi v pravico do zasebnosti so lahko uničujoči že za odrasle, ki želimo obdržati nekatere informacije zase in za tiste, ki jim najbolj zaupamo. Zato nam je neprijetno, ko za naše skrivnosti izve nekdo drug, ki mu to ni namenjeno. Še slabše je v primeru, da nekdo naše skrivnosti uporabi proti nam. Neželena pošta ali preklic zlorabljenе kreditne kartice sta zanemarljivi posledici v primerjavi s krajo denarja, krajo identitete, spletnim nadlegovanjem, izsiljevanjem ali spolnim nadlegovanjem, ki se prav tako lahko posledično zgodi. Stvari se še poslabšajo, če je v navedeno vključen otrok – oseba, ki še ni dosegla zrelosti in je s tem še bolj ranljiva.

1.2. ZAKONI O VAROVANJU ZASEBNOSTI PONUJAJO UNIVERZALNO ZAŠČITO IN OPOLNOMOČENJE POSAMEZNIKOV

K varovanju svoje zasebnosti lahko prispevamo tako, da smo previdni glede lastnih osebnih podatkov. V tem smislu velik del odgovornosti sloni na nas samih. Poleg našega skrbnega ravnanja pa obstajajo tudi zakonske zahteve za tiste, ki upravljajo z našimi osebnimi podatki. Te naj bi nas zaščitile pred zlorabo naših podatkov, saj zavedanje tveganj in pazljivost sama po sebi nista dovolj. Korenine take zakonodaje segajo v leto 1890. Kot odziv na vse večjo priljubljenost in širjenje invazivne uporabe fotografije v medijih, se je v Združenih državah Amerike pojavila ideja zasebnosti kot »pravice, da te pustijo pri miru«, tudi kot odziv na razvoj evropskega prava⁴.

Sodobno pravno varstvo zasebnosti velja univerzalno, to je, za vsakogar. Utemeljeno je predvsem na mednarodnem pravu človekovih pravic, torej na Evropski konvenciji o človekovih pravicah (1950)⁵ in Listini o temeljnih pravicah Evropske unije (2000).⁶ Vzporedno se je varstvo zasebnosti postopoma pojavilo tudi v pravnih redih držav članic Evropske unije. Evropska zakonodaja o varstvu osebnih podatkov določa pogoje in ukrepe za zakonito obdelavo osebnih podatkov, daje posameznikom posebne pravice in predvideva obstoj neodvisnih organov za nadzor.

⁴ S. WARREN in L. BRANDEIS, »Pravica do zasebnosti« (1890) 4 Harvard Law review 5, 193. Cf. Tudi: G.GONZALEZ FUSTER, *Pojav varovanja osebnih podatkov kot temeljne pravice EU*, Springer, Dordrecht 2014.

⁵ Konvencija o varstvu človekovih pravic in temeljnih svoboščin (1950) ETS 5; http://echr.coe.int/Documents/Convention_ENG.pdf, dostopno 20. 5. 2016.

⁶ Listina temeljnih pravic Evropske unije (2000) OJ C 361/1.

Zakonodaja o varovanju zasebnosti predvideva nekaj dejavnosti posameznika. Res je, da so določbe običajno nekoliko pokroviteljske in zelo omejujoče, vendar pa je njihov namen varovanje naših svoboščin, poleg tega pa nam še vedno puščajo veliko manevrskega prostora. V takih primerih skrb za zasebnost pride nazaj v naše roke v smislu opolnomočenja. Kadar imamo izbiro, pa seveda nosimo tudi posledice. Zato smo upravičeni do prejema celovitih in jasnih informacij o obdelavi naših osebnih podatkov. Na primer, pogosto moramo podati soglasje, da se lahko naročimo na brezplačno spletno storitev in se na ta način strinjamo z določenimi postopki obdelave naših osebnih podatkov. Podano privolitev običajno lahko kadarkoli kasneje tudi prekličemo. V teoriji je ta možnost izbire zelo močno orodje v rokah posameznika.

1.3. ZAKONODAJA O VAROVANJU ZASEBNOSTI PREPOZNAVA POMEN POSEBNIH VAROVALK ZA OTROKE

Sodobne otroke zaradi njihove »brezskrbne seznanjenosti«⁷ s tehnološkimi tematikami poimenujemo tudi »digitalni domorodci«⁸, saj informacije uporabljajo bistveno drugače kot njihovi predhodniki.⁹ Uporaba tehnologije je med njimi zelo razširjena in raste. Statistika kaže, da je že leta 2011 več kot 75 % evropskih otrok uporabljalo internet za vrsto namenov, od komuniciranja z vrstniki (posebno na družbenih omrežjih) do nalaganja vsebin (poslušanja glasbe) ali igranja igranic. Nekateri od njih objavljajo vsebine na spletu, npr. pišejo blog¹⁰. Otroci danes na različne načine dostopajo do spleta že v mlajših letih¹¹. Zaradi tega ni presenetljivo, da so vedno bolj v ospredju praks inovativne obdelave podatkov. Vsak dan prinese kakšno inovacijo: aplikacije za pametne telefone, ki merijo porabo mleka ali »pametne ure«, s katerimi mama in oče lahko spremljata, kje so njihovi otroci.¹² Vendar to ne pomeni, da se otroci bolj kot odrasli zavedajo, kaj se dogaja z njihovimi osebnimi podatki, ko so v rokah drugih. Prav tako se ne zavedajo vseh tveganj, povezanih s takimi ravnanji s

⁷ *American Libraries Association v. Pataki* (1997) 969 F. Supp.160.

⁸ M. PRENSKY, 'Digitalne generacije, digitalni priseljenci' (2001). *On the Horizon* 5, 1.

⁹ Ibid.

¹⁰ S. LIVINGSTONE in drugi, *Tveganja in varnost na Internetu: Vidik evropskih otrok*, London School of Economics and Political Science, London 2011, p. 33.

¹¹ S. LIVINGSTONE (ur.), *EU otroci na spletu. Ugotovitve, metode, priporočila*, London School of Economics and Political Science, London, 2015, p.6.

¹² O tej temi glej predvsem: G. GONZALEZ FUSTER, 'GDPR: vsi moramo prispevati k delu!', *Boljši Internet za otroke (BIK) Bulletin*, 31. 3. 2016,

<https://www.betterinternetforkids.eu/web/portal/news/detail?articleId=694148>, dostop 20.5.2016.

podatki in možnih kratkoročnih ali dolgoročnih vplivov takih praks na njihovo življenje.

Zakonodaja o varovanju zasebnosti zagotavlja univerzalno varstvo, ki seveda vključuje tudi otroke. Otroci pa so ranljivi posamezniki. Pogosto ne vedo, kako naj se zaščitijo pred nevarnostmi pri deljenju svojih osebnih podatkov preko sodobnih tehnologij. Pri obdelavi osebnih podatkov otrok so povečana obstoječa tveganja zanje, izpostavljeni pa so tudi novim, zato so pri njih potrebni posebni zaščitni ukrepi. Šele pred kratkim je to prepoznala tudi evropska zakonodaja. Nedavno (aprila 2016) sprejeta reforma okvira varstva podatkov eksplicitno prepoznava potrebo po višji stopnji varstva za ranljive skupine, ki vključujejo otroke. Preambula Splošne uredbe o varstvu podatkov pravi, da

'(...) otroci potrebujejo posebno varstvo v zvezi s svojimi osebnimi podatki, saj se morda manj zavedajo zadevnih tveganj, posledic in zaščitnih ukrepov in svojih pravic v zvezi z obdelavo osebnih podatkov. Tako posebno varstvo bi moralo zadevati zlasti uporabo osebnih podatkov otrok v namene trženja ali ustvarjanja osebnostnih ali uporabniških profilov in zbiranje osebnih podatkov v zvezi z otroki pri uporabi storitev, ki se nudijo neposredno otroku. Privolitev nosilca starševske odgovornosti ne bi smela biti potrebna v okviru storitev preventive ali svetovanja, ki se nudijo neposredno otroku (...)'¹³.

1.4. NEKATERIM TEŽAVAM NA PODROČJU ZASEBNOSTI SE LAHKO IZOGNEMO Z ZAVEDANJEM

Stara modrost pravi, da je bolje preprečiti kot zdraviti. V nekaterih primerih je izvajanje preventivnih ukrepov v celoti v rokah tistih, ki obdelujejo naše osebne podatke. Sami ne moremo kaj dosti storiti, če na primer naš internetni ponudnik postane žrtev hekerskega napada. Zato je odgovornost teh ponudnikov, da zagotovijo ustrezno varnost in zaščito njihovih produktov in storitev.

Včasih pa so primerni ukrepi za preprečitev tveganj in nevarnosti, ali vsaj za zmanjšanje možnosti za njihov nastanek, v naših rokah. Najpreprostejši način je tehten razmislek, preden delimo osebne podatke z drugimi ali privolimo v določeno obdelavo osebnih podatkov.

Moramo pa se najprej zavedati nevarnosti, ki so povezane z obdelavo osebnih podatkov in načinov, kako se pred nevarnostmi zaščititi. Študije kažejo, da velika večina Evropejcev "razkrivanje osebnih podatkov dojema kot del sodobnega

¹³ Uvodna opomba 38; Direktiva (EU) 2016/679 Evropskega parlamenta in Sveta z dne 27.4.2016 o zaščiti fizičnih oseb pri obdelavi osebnih podatkov in o prostem pretoku takšnih podatkov in o razveljavitvi Direktive 95/46/EC (Splošna uredba o varstvu podatkov) (2016) OJ L 119/1.

življenja”, hkrati pa niso dovolj seznanjeni s tem, kako poskrbeti za varstvo podatkov.¹⁴ Posameznike študije običajno prikazujejo kot “neinformirane in zmedene”, zaradi česar si ti pogosto “napačno razlagajo svoje vedenje”.¹⁵ Omenjeno je že bilo, da zakon daje posamezniku možnost privolitve, kar je močno orodje. Toda najbolj običajno na internetu le klikamo “se strinjam”, ne da bi sploh pomislili na možne posledice našega soglasja v obdelavo osebnih podatkov. Statistika kaže, da Evropejci niso dovolj informirani o možnih ukrepih v primerih, ko gre kaj narobe.¹⁶ Še pomembneje, ne zavedajo se niti, da obstajajo nacionalni organi za varstvo osebnih podatkov, ki jim v takih primerih lahko nudijo podporo.¹⁷ Celotni tisti, ki se tega zavedajo, pogosto ne dojemajo nevarnosti v zadostni meri.¹⁸ Povedano enostavno, te nevarnosti se niti ne dotaknejo njihove domišljije: “ne bo se zgodilo meni, to ni zelo verjetno” ali “na to bom mislil šele, ko se mi bo zgodilo.” Toda včasih je preprosto prepozno. Posegi v zasebnost so zaradi nepovratnosti razkritja informacij praviloma nepopravljivi.

Obveščena posameznika še ne pomeni nujno, da bo svojo zasebnost znal ustrezno varovati. Zadostno informirani posamezniki naj bi se zavedali groženj in bi se lahko pravilno odločali. Statistika pa kaže, da v večini primerov niso dovolj informirani. To je še bolj pereče pri otrocih, zlasti zato, ker nedvomno niso v položaju, da bi se odločali informirano in odgovorno, kot odrasli. Veliko napora pogosto vložimo v vztrajanje, da bi se morali otroci, kar zadeva njihovo zasebnost, nehati obnašati kot otroci.

1.5. OPOLNOMOČENJE NAJBOLJ RANLJIVIH

Izobraževanje otrok o zasebnosti mora preseči tako razmišljanje tako, da zajame širšo sliko. Pomembno je otrokom svetovati, naj dvakrat premislijo o tem, kaj počnejo s svojimi osebnimi podatki, poleg tega je pomembno, da otroci vedo, da si njihovi osebni podatki zaslužijo, da jih varujejo tudi drugi. Pravilna odločitev pri razkrivanju osebnih podatkov je ključni element varstva zasebnosti, toda ni

¹⁴Evropska komisija, *Special Eurobarometer 359: Attitudes on Data Protection and Electronic Identity in the European Union*, Bruselj 2011, str. 5,

http://ec.europa.eu/public_opinion/archives/ebs/ebs_359_en.pdf, dostopno 20.05.2016.

¹⁵G. GONZÁLEZ FUSTER, ‘How Uninformed Is the Average Data Subject? A Quest for Benchmarks in EU Personal Data Protection’ (2014) 19 *IDP. Revista de Internet, Derecho Y Política*, 99.

¹⁶Evropska agencija za temeljne pravice, *Access to Data Protection Remedies in EU Member States*, Publications Office of the European Union, Luksemburg 2014, str. 32–34.

¹⁷Evropska komisija, *Special Eurobarometer 359*, op. cit., str. 174.

¹⁸J.B. RULE, *The Politics of Privacy: Planning for Personal Data Systems as Powerful Technologies*, Elsevier, New York 1980, str. 184.

edini. Poučevanje otrok naj ne prispeva le k njihovi varnosti, pač pa naj jim tudi daje moč; to gre z roko v roki.

Opolnomočen posameznik se bo bolj uspešno zaščitil pred težavami s posegi v zasebnost. Biti poučen pomeni zavedati se nevarnosti, in tudi zavedati se pravic in pravil, ki so na voljo, ter predvidenih načinov za odpravo težav. In če so otroci poučeni, ne bodo poznali le kršitev zasebnosti in tveganj na internetu, temveč tudi to, do česa so upravičeni, kdo je dolžan kaj storiti, ter končno, kako bodo bolj varni.

Prenovljeni pravni okvir v EU, ki izrecno priznava potrebo po posebnem varstvu otrok in vrednost dvigovanja zavedanja o zasebnosti, lahko vzamemo za zgled. Prav tako morajo nadzorni organi posvečati posebno pozornost otrokom. Ti organi, običajno imenovani "nadzorni organi za varstvo osebnih podatkov" so ključni sestavni del temeljne pravice do varstva osebnih podatkov in imajo glede na zakonodajo veliko različnih nalog.

Zgodovinsko gledano so nadzorni organi od začetka svojega obstoja v 70. letih pooblašteni ne le za nadzor nad spoštovanjem predpisov o varstvu osebnih podatkov, temveč jim je bil zaupan širok del drugih nalog, od vloge nekakšnega ombudsmana, "revizorja", svetovalca in do sooblikovalca pri pripravi politik na tem področju.¹⁹ Ena od nalog je tudi izobraževanje javnosti. Vse te aktivnosti pa imajo skupen cilj – doseči višjo raven varstva osebnih podatkov.

V predpisih se je postopoma odrazila razširitev poslanstva nadzornih organov. Novo sprejeta Splošna uredba o varstvu osebnih podatkov, ki bo začela veljati maja 2018, jim izrecno podeljuje določene naloge. Tako 57. člen uredbe med drugim določa:

'da vsak nadzorni organ na svojem ozemlju [...]spodbuja ozaveščenost in razumevanje javnosti o tveganjih, pravilih, zaščitnih ukrepih in pravicah v zvezi z obdelavo. Posebna pozornost se posveti dejavnostim, ki so namenjene izrecno otrokom.'

Splošna uredba o varstvu osebnih podatkov tako izrecno priznava, da morajo otroci poznati tveganja, povezana z obdelavo osebnih podatkov, ter da morajo poznati tudi pravila v zvezi s tem, zaščitne ukrepe in pravice. Zavedanje o

¹⁹C.J. BENNETT in C.D. RAAB, *The Governance of Privacy: Policy Instruments in Global Perspective*, MIT Press, Cambridge 2006. Za pregled glej tudi: Evropska komisija, *Evaluation of the Means used by National Data Protection Supervisory Authorities in the promotion of personal Data Protection. Final Report*, Bruselj 2009.

tveganju je pravzaprav ključnega pomena za to, da otroci svoje pravice tudi koristno uporabljajo.

Vredno je omeniti, da je dvigovanje zavesti o varstvu zasebnosti med otroki tematika, ki je prisotna tudi izven meja EU. Tako so bile na primer Združene države Amerike začetnice na področju urejanja varstva zasebnosti na internetu s tem, ko so leta 1998 sprejele Zakon o varstvu zasebnosti otrok na internetu,²⁰ ki se nanaša na spletne strani, ki zbirajo informacije od otrok, mlajših od 13 let. Zvezna komisija za trgovino v ZDA, ki je udeležena pri izvrševanju zakona, upravlja različne spletne strani, ki skušajo dvigovati ozaveščenost med otroki.

2. PREGLED STANJA NA PODROČJU IZOBRAŽEVANJA O ZASEBNOSTI V EVROPI

V projektu ARCADES smo pregledali mnoge aktivnosti za poučevanje otrok o zasebnosti v evropskih šolah in zaznali njihovo raznolikost.²¹ Projekt je bil osredotočen na analizo dostopnega izobraževalnega gradiva.

2.1. KDO?

Pripravljalce smernic in konkretnega gradiva za poučevanje zasebnosti v šolah lahko ločimo glede na njihov izvor in glede na pristop k problematiki varstva zasebnosti. Mednarodne organizacije, kot je na primer Organizacija združenih narodov za izobraževanje, znanost in kulturo (UNESCO)²², so bile ustanovljene tudi z namenom varovanja pravic otrok in s tem njihove pravice do zasebnosti. Enako velja za Svet Evrope, ki se prav tako ukvarja z izobraževanjem o zasebnosti z vidika človekovih pravic. Evropska unija deluje na tem področju tako z vidika varnosti na internetu kot tudi z vidika temeljnih človekovih pravic.

Nadzorni organi za varstvo osebnih podatkov so prav tako dejavni na tem področju; njihove kampanje za ozaveščanje so ponekod usmerjene neposredno k otrokom (na primer prek spletne strani), lahko pa tudi k staršem ali učiteljem. Nekateri ponujajo, da njihovi strokovnjaki predavajo na šolah. Veliko vlog

²⁰ Children's Online Privacy Protection Act of 1998, 5 U.S.C. 6501–6505.

²¹ G. GONZÁLEZ FUSTER, P. DE HERT in D. KLOZA, *State-of-the-Art Report on Teaching Privacy and Personal Data Protection at Schools in the European Union*, Vrije Universiteit Brussel, Bruselj 2015, <http://arcades-project.eu/images/pdf/State_of_the_art_report.pdf> dostop 25.05.2016.

²²O tem glej zlasti: P. HLADSCHIK in D. STEURER, 'Human Rights Education – Know Your Rights!' in M. NOWAK, K.M. JANUSZEWSKI in T. HOFSTÄTTER (ur.) *All Human Rights for All: Vienna Manual on Human Rights*, Intersentia, Dunaj/Graz 2012, str. 606-612.

igrajo organizacije civilne družbe, ki aktivno sodelujejo pri izobraževanju in ponujajo učne pripomočke. Vprašanje vključevanja izobraževanja o zasebnosti v nacionalne učne načrte pa ne nazadnje sodi v pristojnost države, pri čemer še niso vse članice EU naredile koraka v to smer. Jasno pa je, da pri spodbujanju poučevanja o zasebnosti v šolah aktivno sodelujejo različni deležniki.

Otroci so običajno glavna ciljna skupina izobraževalnih dejavnosti, lahko pa so programi zasnovani tudi tako, da so usmerjeni k učiteljem. Občasno programi za poučevanje o zasebnosti aktivno vključujejo tudi starše, ob upoštevanju, da so prav oni ključni dejavnok varovanja otrokove zasebnosti, in da je k njim najboljše pristopiti prek šole.

2.2. KJE IN KDAJ?

Poučevanje o zasebnosti se lahko izvaja na vseh ravneh izobraževanja. Čeprav se v nekaterih državah EU pojavlja že v učnih načrtih za vrtce, se na splošno tovrstno izobraževanje izvaja v osnovnih in srednjih šolah.

Prizadevanja za izobraževanje v šolah seveda niso edini način, kako dvigniti ozaveščenost o varovanju zasebnosti med otroki. Otroke, starše in učitelje je mogoče doseči tudi prek medijev, bodisi tradicionalnih (npr. televizija ali časopisi), bodisi novejših (npr. spletne strani). Vrsto aktivnosti organizirajo na javnih mestih (npr. v knjižnicah ali na izobraževalnih seminarjih), obstajajo pa tudi posebni dogodki (npr. Dan varne rabe interneta).

2.3. KAKO?

V tistih državah članicah EU, kjer izobraževanje o zasebnosti predstavlja del formalne šolske izobrazbe, je v učne načrte vključeno na različne načine, npr. med tematike poznavanja temeljnih pravic ali računalniške pismenosti in odgovorne uporabe informacijsko komunikacijskih tehnologij. Splošno znanje o temeljnih pravicah otroci navadno pridobijo v okviru »državlanske vzgoje«, o uporabi informacijske tehnologije pa se učijo v okviru »računalništva« ali »medijev«. Seveda je poimenovanje predmetov različno od države do države.

Izobraževanje o varovanju zasebnosti podpirajo tudi nadzorni organi za varstvo osebnih podatkov kot del svojih aktivnosti za dvig ozaveščenosti, ki so namenjene neposredno ali posredno otrokom, večinoma prek njihovih staršev in učiteljev ter strokovnjakov s področja izobraževanja, ki naprej vplivajo na otroke.

Nadzorni organi za varstvo osebnih podatkov nudijo predvsem spletne vsebine (npr. posebne spletne strani in gradiva), organizirajo promocijske kampanje in tekmovanja. Svojo izobraževalno dejavnost še posebej okrepijo v času posebnih dogodkov in praznikov, denimo Evropskega dneva varstva osebnih podatkov (28. januar). Občasno se njihovi predstavniki udeležijo posebnih sejmov in dni odprtih vrat v šolah ter knjižnicah.

Predstavniki nadzornih organov tudi neposredno sodelujejo pri izobraževanju o zasebnosti, tako da obiščejo šole ali se udeležujejo drugih dogodkov, npr. predavanj, seminarjev ali delavnic, ob posamičnih priložnostih ali kot stalno aktivnost. Udeležba na tovrstnih dogodkih je praviloma brezplačna. Veliko nadzornih organov je že izdalo oziroma redno izdaja brezplačno izobraževalno gradivo za otroke v elektronski ali fizični obliki, in obsega posebne spletne strani, plakate, voščilnice, brošure, letake, stripe, video posnetke, kvize, smernice in celo učne načrte.

Nadzorni organi za varstvo osebnih podatkov med seboj sodelujejo na evropski in na mednarodni ravni. Delovna skupina iz člena 29, svetovalno telo, ki ga sestavljajo predstavniki vseh nadzornih organov za varstvo osebnih podatkov držav članic EU, je leta 2009 izdala pomembno mnenje o varstvu osebnih podatkov otrok²³. Na 35. Mednarodni konferenci pooblaščenec za zasebnost in varstvo osebnih podatkov (v Varšavi 2013) je bila sprejeta tudi resolucija o Digitalni izobrazbi za vse²⁴, kar je zagnalo delo Mednarodno delovne skupine za varstvo osebnih podatkov in digitalno izobraževanje. Vzporedno s temi dejavnostmi posamezni nadzorni organi za varstvo osebnih podatkov redno organizirajo študijske obiske in izmenjavo zaposlenih z namenom deljenja izkušenj in dobrih praks.

Nadzorni organi za varstvo osebnih podatkov ne sodelujejo le s šolami, pač pa tudi z drugimi organi in institucijami, denimo z občinskimi sveti in knjižnicami. Francoski nadzorni organ za varstvo osebnih podatkov je vodil skupino za

²³ Delovna skupina iz Člena 29, *Mnenje 2/2009 o varstvu osebnih podatkov otrok (Splošne smernice in poseben primer šol)*, WP 160, Bruselj, 11. 2. 2009. <http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp160_en.pdf> dostop 25. 5. 2016. Predhodno k temu mnenju: Idem, *Delovni dokument 1/2008 2009 o varstvu osebnih podatkov otrok (Splošne smernice in poseben primer šol)*, WP 147, Bruselj, 18. 2. 2008 http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2008/wp147_en.pdf, dostopno 25. 5. 2016.

²⁴ Mednarodna konferenca pooblaščenec za zasebnosti in varstvo osebnih podatkov, Resolucija o digitalni izobrazbi za vse (2013) <<https://icdppc.org/wp-content/uploads/2015/02/Digital-education-resolution.pdf>> dostopno 20. 5. 2016.

digitalno izobraževanje »EducNum«, ki je k sodelovanju privabila več kot šestdeset institucij s področja izobraževanja, digitalne ekonomije, civilne družbe in politike ter raziskovalnih organizacij²⁵. Dejavnosti nadzornih organov za varstvo osebnih podatkov so lahko usmerjene tudi k vplivanju na razvoj politik, npr. z namenom oblikovanja šolskega učnega načrta ali svetovanja političnim odločevalcem. Pogosto se pri tem oprejo na rezultate raziskav, ki merijo stopnjo zaznane ogroženosti med otroki.

Mednarodna in nadvladna telesa postavljajo standarde na področju izobraževanja o zasebnosti, prav tako pa neposredno sodelujejo pri izvajanju izobraževalne dejavnosti. Tako je na primer Svet Evrope ob 50. obletnici Evropske konvencije o človekovih pravicah vzpostavil »COMPASS«, digitalno orodje, s katerim zasleduje cilj razvoja znanja, spretnosti in odnosa do človekovih pravic. Ena od tem v omenjenem kontekstu so pravice otrok²⁶. Leta 2007 je Svet Evrope prvič izdal priročnik o internetni pismenosti²⁷, zdaj že v tretjem ponatisu, leta 2012 pa je pripravil Strategijo za pravice otrok (2012-2015)²⁸.

Prizadevanja EU za izobraževanje o zasebnosti so bila v okviru programa »Varni internet« leta 1999 finančno podprta s proračunom 50 milijonov EUR. Leta 2012 je bila sprejeta Evropska strategija za otrokom prijazen internet²⁹, oz. krajše »Boljši internet za otroke«. Strategija, sicer zasnovana na štirih stebrih, glede »dvisa ozaveščenosti in možnosti odločanja«, ugotavlja,

da se morajo otroci, njihovi starši, skrbniki in učitelji zavedati tveganj, ki prežijo na otroke na internetu, prav tako pa tudi orodij in strategij, ki omogočajo zaščito in upravljanje s tveganji.³⁰

Strategija še poudarja pomen veščin digitalne in medijske pismenosti, ki je ključna za otroke na spletu. Prav tako poudarja, da je »z izobraževanjem o spletni

²⁵ <http://www.educnum.fr>, dostopno 18. 5. 2016.

²⁶ <<http://www.eycb.coe.int/compass>> dostop 18. 5. 2016.

²⁷ Svet Evrope, Priročnik o internetni pismenosti, 3. izdaja., Strasbourg 2007, http://www.coe.int/t/dghl/StandardSetting/InternetLiteracy/InternetLiteracyHandbook_3_EN.asp, dostop 26. 5. 2016.

²⁸ Svet Evrope, Strategija o pravicah otrok (2012-2015), CM(2011)171 končna, Strasbourg, 15.02.2012, <http://www.coe.int/t/DGHL/STANDARDSETTING/CDcj/StrategyCME.pdf>, dostop 26. 5. 2016.

²⁹ Evropska komisija, Evropska strategija za boljši internet za otroke, COM(2012) 196 končna, Bruselj, 2. 5. 2012.

³⁰ Ibid., str. 8.

varnosti treba začeti v zgodnjem otroštvu³¹«. Glede na to, da je spletna varnost kot posebna tema vključena v učne načrte več kot 20 izobraževalnih sistemov v Evropi, strategija pravi,

‘da so šole tiste, ki lahko najbolje dosežejo večino otrok, ne glede na starost, dohodek ali družbeno ozadje pa tudi druge posameznike, npr. učitelje in (posredno) starše’.³²

Zato so bile države članice EU pozvane, da do leta 2013 v šolske učne načrte vključijo izobraževanje o spletni varnosti, da okrepijo neformalno izobrazbo s tega področja, da vzpostavijo ustrezne politike »spletne varnosti« in poskrbijo za usposabljanje učiteljev, tudi s pomočjo javno-zasebnih partnerstev. K sodelovanju pri razvoju interaktivnih orodij in platform, ki so namenjene predstavitvi izobraževalnega gradiva za učitelje in starše, je bilo povabljen tudi gospodarstvo. Evropska komisija se je še posebej zavezala k podpori formalnemu in neformalnemu izobraževanju s področja spletne varnosti. Vendar pa se izobraževanje »o zasebnosti« z vidika spletne varnosti usmerja predvsem k dvigu ozaveščenosti o grožnjah, ki na otroke prežijo na spletu. Ni pa zadostnega poudarka na dvigu ozaveščenosti glede temeljnih pravic in njihove večrazsežnosti.

2.4. KAJ?

Poglavitna značilnost pregledanega izobraževalnega gradiva je, da ne cilja zgolj na prenos znanja, pač pa skuša spodbujati učenje in premislek. Temeljni cilj je krepitev premišljene in odgovorne uporabe razvijajoče se informacijsko komunikacijske tehnologije, še posebej interneta. Izobraževalna gradiva niso usmerjena le na področje varstva zasebnosti, pač pa se pogosto prekrivajo še s področjem spletne varnosti in varnostnih izzivov, kar naj bi krepilo določeno mero »digitalne odgovornosti«.

Izobraževalna gradiva praviloma skušajo:

- razjasniti, kaj je »zasebnost«, v nekaterih primerih tudi kaj je »nadzor«,
- poudariti velik pomen teh konceptov v sodobni družbi,
- ponuditi razmislek o tem, ali naj se sploh odločimo za deljenje svojih osebnih podatkov ali ne,

³¹ Ibid.

³² Ibid.

- če se že odločimo za deljenje svojih osebnih podatkov, skušajo:
 - ponuditi predloge o tem, kako si zagotoviti varnost na spletu, npr. z izbiro ustreznega gesla ali s spremembami nastavitve zasebnosti na družbenih platformah,
 - razložiti, kako naj podamo veljavno privolitev glede deljenja svojih podatkov (še posebej to velja za otroke) in kako prekličemo to privolitev,
 - pojasniti, da je podatke, ko se enkrat pojavijo na spletu, težko umakniti (gre za idejo, da internet »nikoli ne pozabi«),
 - nuditi pomoč v zvezi s pravicami, ki jih imamo, npr. da se lahko obrnemo na nadzorne organe za varstvo osebnih podatkov,
- nakazati vlogo staršev pri zagotavljanju varstva osebnih podatkov otrok.

Glavni namen tovrstnih izobraževalnih akcij sicer ni vselej jasen. V nekaterih primerih je poudarek na učenju otrok o tem, kako naj zavarujejo svojo zasebnost in razširijo poznavanje temeljnih pravic, ki jim pripadajo. V drugih primerih pa je poudarek na tem, da otroke odvrčamo od izpostavljanja tveganjem, kar je v bistvu ravno nasprotno temu, da jim skušamo razložiti, katere pravice imajo in da morajo upravljalci osebnih podatkov te pravice spoštovati.

Spodnja tabela kaže ključne točke procesa (kdo, komu, kje, kako in kaj) izobraževanja otrok v EU o zaščiti zasebnosti.

Tabela 1 – hitri pregled področja izobraževanja o zasebnosti

Kdo?	Komu?	Kam?	Kako?	Kaj?
- regulatorji	- otrokom	- vrtci	- uradni učni načrti	- opredelitve
• vlade	- staršem	- šole:	- posredno	- pomen
• nadnacionalne organizacije	- učiteljem	osnovne,	• gradiva za učitelje	- pravice
• mednarodne organizacije	- skrbnikom	srednje,		- sredstva za obrambo
- oblikovalci standardov		višje		- varnostni namigi
- nadzorni organi za varstvo osebnih podatkov		- mediji	• gradiva za starše	
- nevladne organizacije		- javni prostori	- neposredno	
- gospodarstvo		- javni dogodki	• gradiva za otroke	

3. ZAKLJUČNE MISLI

Teža izzivov varstva zasebnosti je pogosto podcenjena. Slabo je že, če postane žrtev tega odrasel človek, če pa se zgodi otroku, je škoda še večja. Otroci so posebej ranljivi zaradi svoje pomanjkljive ozaveščenosti o nevarnostih, povezanih z uporabo tehnologije. Zato jih je treba dodatno zaščititi. Hkrati pa so otroci »digitalni domorodci«, ki se na videz brez težav znajdejo v digitalnem svetu.

Varstvo zasebnosti se začne s tem, da vsak posameznik najprej poskrbi zase. Šele potem nastopi pravo z naborom ukrepov, ki zagotavljajo relativno visok nivo zaščite, hkrati pa dopuščajo posamezniku dosti svobode pri odločitvah, npr. tako, da se lahko sam odloči, kdaj bo in ali bo podal privolitev za obdelavo osebnih podatkov. Vendar pa se mora posameznik najprej zavedati različnih nevarnosti in načinov, kako v takih primerih ustrezno ravnati. Otroci, starši in učitelji se lahko relativno uspešno soočajo z izzivi glede zasebnosti, če imajo dovolj ustreznega znanja. Vendar se ne smemo slepiti, da bo za zaščito zasebnosti otrok poskrbljeno, če jih zgolj opozarjamo, naj pred vsako odločitvijo dvakrat premislijo, oziroma, da bi že morali vedeti, kaj se bo zgodilo, če ne bodo previdni. Če bi otroci že vedeli, kaj se bo zgodilo, najbrž ne bi bili več otroci.

Zato je pomemben širok pristop k izobraževanju o varstvu zasebnosti, katerega namen ni zgolj reševanje problemov v zvezi z zasebnostjo oziroma dvigovanje ozaveščenosti. Treba je doseči tudi, da se bodo otroci zavedali pravic, ki jih imajo, ter pravil, ki jih morajo v zvezi z obdelavo osebnih podatkov spoštovati upravljavci. Gre za nekakšno opominjanje o razsežnosti zasebnosti, ki se v svojem bistvu dotika temeljnih človekovih pravic. Otroci naj pomena zasebnosti ne bi poznali le zato, da bodo varni, pač pa zlasti zato, da se bodo lahko razvijali kot svobodni posamezniki.

Izobraževanje o zasebnosti je v evropskih šolah že dlje prisotno, splošno je priznana tudi pomembnost le-tega. Dosedanje delo različnih organizacij je vsekakor treba pohvaliti, vendar je treba storiti še več. Zaradi svojega strokovnega znanja in izkušenj imajo ključno vlogo pri spodbujanju in izboljševanju izobraževanja o zasebnosti v šolah nadzorni organi za varstvo osebnih podatkov. Opazno lahko prispevajo k dvigu kvalitete, denimo tako, da preverijo, ali so informacije, ki jih podajajo v šolah, v celoti skladne z zahtevami aktualne zakonodaje.

Primer dobre prakse je Splošna uredba o varstvu osebnih podatkov, s katero so nadzorni organi varstvo osebnih podatkov postali formalno zavezani k

ozaveščanju javnosti o varstvu osebnih podatkov in zasebnosti. Dodatno pozornost je treba nameniti otrokom, saj so zaradi ranljivosti bistveno bolj izpostavljeni tovrstnim tveganjem.

Otrok ne smemo podcenjevati, vendar v celoti tudi ne prepuščati samim sebi, ko se gibajo po digitalnem svetu s številnimi spolzkimi cestami. Njihovo »digitalno domorodnost« bi bilo treba dopolniti in uravnotežiti z »digitalno odgovornostjo«. Šola in dom sta najprimernejši mesti za to, saj jih tam obravnavamo kot otroke in hkrati kot subjekte varstva osebnih podatkov.

Izobraževanje ni čudežna paličica za rešitev vseh težav v zvezi z zasebnostjo. Varovanje zasebnosti otrok namreč zahteva še veliko več, med drugim tudi prilagojene informacije in stroga pravila za obdelavo otrokovih osebnih podatkov. Kljub temu pa je izobraževanje pomemben košček sestavljanke v zapleteni pokrajini zasebnosti.

II. DEL
PRIROČNIK ZA UČITELJE

PREDSTAVITEV PRIROČNIKA ZA UČITELJE

Namen in smisel tega priročnika je, da postane uporabno gradivo za učitelje katerekoli šole v EU, ki bi želela učence in dijake poučiti o zasebnosti in varstvu osebnih podatkov. V želji, da bi bil priročnik uporaben na celotnem območju EU, ponuja informacije, ki so relevantne v vseh državah članicah EU in temeljijo na veljavnih evropskih pravnih aktih, zlasti na Listini EU o temeljnih pravicah. Glede posebne pravne ureditve v posamezni državi članici pa se lahko učitelji vedno obrnejo na nacionalne organe za varstvo osebnih podatkov, v Sloveniji torej na Informacijskega pooblaščenca.

Priročnik je napisan v jeziku, ki bo učiteljem pomagal najti prave izraze za razlago tematike. Sestavljen je iz desetih poglavij, ki pokrivajo različne vidike zasebnosti in varstva osebnih podatkov, pomembne za otroke in najstnike. Vsako od poglavij vsebuje ključne poudarke obravnavane teme, predlagane iztočnice za pogovor z otroki, priporočene dejavnosti v razredu ter konkretne nasvete za otroke na področju zasebnosti in varstva osebnih podatkov. Poglavja ponujajo tudi primere in zgodbe iz dejanskega življenja, ki lahko učencem približajo posamezno tematiko. Na koncu vsakega poglavja priročnik izpostavlja ključne poudarke, ki so pomembni za najmlajše, ter tiste poudarke, ki so namenjeni starejšim otrokom oziroma najstnikom. Učitelje vabimo, da se seznanijo s priročnikom kot celoto, nato pa lahko iz njega poljubno in po lastni presoji uporabljajo elemente posameznih poglavij v skladu s potrebami in učnimi cilji v razredu.

Avtorji priročnika in grafičnih elementov so (v abecednem redu): Viktor Árvay (NAIH), Jelena Burnik (IP RS), Paul De Hert (VUB), Piotr Drobek (GIODO), Gloria González Fuster (VUB), Urszula Góral (GIODO), Dariusz Kloza (VUB), Laura Kozma (NAIH), Paweł Makowski (GIODO), Marta Mikołajczyk (GIODO), Kata Nagy (NAIH), Anže Novak (IP RS), Zsófia Szántó (NAIH), Julia Sziklay (NAIH), Polona Tepina (IP RS) and Zsófia Tordai (NAIH).

1. O ZASEBNOSTI

Kaj je zasebnost? Zakaj je pomembna?

CILJI

To uvodno poglavje naj bi učencem pomagalo:

- spoznati, kaj je zasebnost;
- oblikovati kritičen odnos do zasebnosti;
- razumeti pomen zasebnosti v "resničnem" svetu ter na spletu.

KLJUČNI POUČENKI

Zasebnost po eni strani predstavlja tisto, kar je za človeka **intimno**, hkrati pa predstavlja možnost "**biti sam svoj**" in imeti možnost živeti v skladu s svojimi željami in potrebami ter svobodno oblikovati svoje cilje in prioritete. Pravica do **zasebnosti** pomeni možnost zaščititi se pred pogledi tretjih, prav tako pa pomeni sposobnost zavrniti posege tretjih v zasebno sfero, bodisi s strani države, staršev, prijateljev, učiteljev ali popolnih neznancev.

Tudi psihologi, ne le pravniki in država, poudarjajo pomen zasebnosti, ki jo lahko prepoznamo v dveh različnih sferah človekovega udejstvovanja. Prva je sfera intimnosti, pri kateri čutimo potrebo po ohranjanju svoje zasebnosti na ravni telesa, čustev in občutij. Na drugi strani pa imamo javno sfero, ki zajema človekovo delovanje in izražanje v javnosti, pri katerem pa prav tako nastopa potreba po ohranjanju določene mere zasebnosti. Obe sferi zasebnosti sta pomembni in potrebni za ohranjanje lastne vrednosti ter za zaščito posameznikove podobe v družbi in odnosih na splošno.

Otroštvo je edinstveno obdobje v življenju vsakega človeka, v katerem je varstvo zasebnosti še posebej pomembno. Vsi otroci, ne glede na to, kje živijo, imajo pravico do življenja in razvoja, odraščanja v okolju, ki spoštuje svobodo in dostojanstvo, in do **zasebnosti** in do **varovanja osebnih podatkov**.

Zasebnost je vedno igrala pomembno vlogo v delovanju **sodobnih demokracij** in je priznana kot **človekova pravica**. Njena vloga je postala posebej izrazita po drugi svetovni vojni kot odgovor na totalitarne režime. Pravica do zasebnosti je priznana v vseh evropskih pravnih sistemih kot tudi v širšem mednarodnem okolju, praviloma kot temeljna človekova pravica. Države ne smejo posegati v

pravico do zasebnosti, hkrati pa morajo zagotoviti učinkovito zaščito te pravice pred posegi tretjih, npr. pred posegi zasebnih podjetij.

Listina Evropske unije o temeljnih pravicah v 7. členu zagotavlja pravico do spoštovanja zasebnega in družinskega življenja.

Sodobne tehnologije predstavljajo poseben izziv za varovanje zasebnosti. Čedalje več komuniciramo, delamo, se učimo in se zabavamo z uporabo tehnologije, tako rekoč **živimo z in skozi tehnologijo**. Vsi ljudje – tudi otroci – morajo torej imeti možnost uživati zasebnost kadarkoli, tudi **na spletu**.

PRIMERI IZ RESNIČNEGA ŽIVLJENJA

Znane osebe so še posebej dovzetne za posege v njihovo pravico do zasebnosti. Mediji vedo, da objava smešnih in nepričakovanih fotografij iz življenja znanih, ki bi jih lahko spravile tudi v zadrego, pritegne veliko radovednih pogledov. Tako imenovani '**paparaci**' preživijo ure in ure v upanju, da bodo ujeli pravi trenutek in posneli dobro fotografijo slavne osebe. A tudi znani ljudje imajo pravico do zasebnosti in mediji zato nimajo pravice do objave fotografij, ki niso v javnem interesu (npr. prikazujejo le običajno preživljanje vsakdanjika slavne osebe) ali do razkritja okoliščin iz zasebnega življenja, ki bi jih znane osebe želele zadržati zase (npr. obisk zdravnika). Veliko medijsko prepoznavnih oseb se je že borilo proti objavi svojih fotografij v medijih, vključno z igralci, manekenkami in princesami.

IDEJE ZA POGOVOR

Z učenci lahko začnete pogovor o naslednjih temah:

1. **Osebnostne izkušnje:** Ali je tudi tebi že kdo posegel v zasebnost? Kaj se je zgodilo? Kako si se na to odzval?
2. **Oblikovanje kritičnega odnosa:** Si lahko predstavljaš družbo, kjer ne bi bilo nobene zasebnosti? Bi si želel živeti v njej? Si lahko zamisliš težave, ki bi v taki družbi nastale? Poskušaj si zamisliti kategorije oseb s posebnimi potrebami po zasebnosti: osebe z zdravstvenimi težavami, ki jih ne želijo deliti z drugimi; novinarji, ki želijo skrito preiskovati družbene probleme; učitelji, ki želijo obdržati razdaljo med sabo in učenci; ljudje, ki se želijo politično udejstvovati in si ne želijo kritik nasprotnikov, ipd.

PRIPOROČENE DEJAVNOSTI

1. Ta vaja lahko učencem pomaga razmišljati o tem, kaj je zasebnost in kaj jo sestavlja, zakaj v določenih situacijah potrebujemo "več zasebnosti" kot v drugih ter o tem, kako se počutimo, ko nekdo poseže v našo zasebnost.
 - Vsi učenci v razredu naj drug drugega pozdravijo tako, kot da se niso videli že več mesecev.
 - Pri tem naj učenci **opazujejo** različne načine pozdravljanja in **premislijo** o naslednjih vprašanjih: Se prijatelji pozdravijo na enak način, kot se pozdravijo znanci? Bi družinskega člana pozdravili na drugačen način? Kako se pozdravijo neznanci? Kako bi se počutili, če bi te želel neznanec pozdraviti na preveč vsiljiv ali preveč "topel" način?
2. Z namenom raziskovanja različnih dimenzij zasebnosti napišite na tablo besedo 'zasebnost' in povabite učence, da **narišejo miselni vzorec**, v katerega vpišejo pojme, povezane z zasebnostjo. Najprej zapišite vse besede, ki so povezane z zasebnostjo, nato pa te besede povežite v skupine, ki se nanašajo na posamezne dimenzije zasebnosti (npr. intimnost telesa, zasebnost komunikacij ipd.).

ZA NAJMLAJŠE

Mlajši učenci se morajo naučiti, da zasebnost pomeni, da je dobro določene stvari zadržati zase, hkrati pa imeti prostor, da smo takšni, kot si želimo biti. Otroci morajo vedeti, da **imajo pravico, da drugi spoštujejo njihovo zasebnost** in da **morajo tudi oni spoštovati zasebnost drugih**.

ZA STAREJŠE IN/ALI BOLJ ZRELE

Starejši učenci morajo razumeti, da je pravica do zasebnosti **temeljna pravica**, ki igra ključno vlogo pri delovanju demokratične družbe. S to pravico so začrtane meje posegov države v življenja posameznikov, zaradi česar lahko živimo svobodno.

2. O VARSTVU OSEBNIH PODATKOV

Kaj so osebni podatki? Kaj pomeni, da imamo pravico do varstva osebnih podatkov?

CILJI

To poglavje naj bi učencem pomagalo:

- razumeti pomen **varstva osebnih podatkov**;
- naučiti se prepoznati '**osebne podatke**' in razumeti, zakaj jih je treba varovati;
- spoznati pojem '**občutljivih podatkov**', oziroma podatkov, ki potrebujejo posebno zaščito;
- povečati ozaveščenost o **pravica**h, ki v zvezi z osebnimi podatki pripadajo vsakemu posamezniku.

KLJUČNI POUČENI

Poleg zagotavljanja pravice do zasebnosti pravo posameznikom zagotavlja tudi **pravico do varstva osebnih podatkov**. Sodobne družbe tej pravici priznavajo status temeljne človekove pravice, predvsem zaradi hudih posledic za življenje posameznika, ki jih lahko povzroči zloraba osebnih podatkov, na primer, ko se določeni podatki pripišejo napačni osebi ali kadar določena organizacija pridobi preveč podatkov o posameznikih.

Prvi zakoni s področja varstva osebnih podatkov so bili sprejeti v **70. letih prejšnjega stoletja**, ko so države in različne gospodarske družbe za shranjevanje in obdelavo podatkov o posameznikih začele uporabljati računalnike. Pojavili so se namreč strahovi, da bi z uvedbo računalnikov tisti, ki razpolagajo s podatki, nad posamezniki pridobili preveliko moč. Posamezniki pa so imeli po drugi strani vedno manj nadzora nad tem, kaj se z njihovimi podatki dogaja. Danes je obdelava osebnih podatkov veliko bolj razširjena, kot bi si v preteklosti sploh lahko zamislili, s čimer je postala pravica do varstva osebnih podatkov še posebej pomembna.

Listina Evropske unije o temeljnih pravicah zagotavlja pravico do varstva osebnih podatkov v 8. členu.

Skozi to pravico pravo ščiti vse ‘**osebne podatke**’, torej vse podatke, digitalne ali analogne, ki jih lahko **povežemo s posameznikom**. To so lahko dokumenti in druge informacije v pisni obliki, slike, video posnetki in celo zvočni posnetki. Osebni podatek je lahko telefonska številka, elektronski naslov, celo nakupovalni seznam, če lahko te podatke povežemo s konkretnim posameznikom. Tudi če je podatek na prvi pogled videti nepomemben in nezanimiv, ga moramo šteti za osebni podatek, ki si zasluži pravno varstvo. Skupek ali povezava različnih, na prvi pogled nepomembnih podatkov lahko namreč vodi do razkritja pomembnih podatkov o osebi, zato pravo ščiti vse podatke, ki štejejo za osebne podatke, na splošno in v celoti.

Poleg tega pravo razlikuje med običajnimi in posebej **občutljivimi podatki**, ki si zaslužijo posebno varstvo. Občutljivi osebni podatki so denimo podatki, ki se nanašajo na posameznikovo politično ali versko **prepričanje**, njegovo **zdravstveno stanje**, **narodno ali narodnostno poreklo** ali njegovo **spolno življenje**. Ti podatki so deležni posebne zaščite zato, da bi preprečili možnost diskriminacije in stigmatizacije posameznikov na podlagi teh lastnosti, pa tudi zato, da se jim omogoči, da zadržijo te podatke zase, če tako želijo.

Z namenom preprečevanja zlorabe osebnih podatkov daje pravo posamezniku, na katerega se nanašajo osebni podatki, **vrsto pravic**. V zakonu so določene **dolžnosti** tistih, ki želijo pridobiti in nadalje obdelovati osebne podatke posameznikov. Za nadzor nad spoštovanjem pravic obstajajo **neodvisni nadzorni organi za varstvo osebnih podatkov**, v Sloveniji je to Informacijski pooblaščenec.

Prav vsi imamo glede svojih osebnih podatkov pravico:

- do informacije o tem, **kdo** obdeluje naše osebne podatke, **katere podatke** obdeluje in **za kakšen namen** (‘pravica do obveščенosti’);
- **vprašati** tiste, ki osebne podatke obdelujejo, da nas seznanijo s tem, katere naše podatke obdelujejo (‘pravica do seznanitve’);
- zahtevati **dopolnitev oz. popravek** nepopolnih, netočnih ali neažurnih osebnih podatkov (‘pravica do popravka’);
- zahtevati **izbris** osebnih podatkov, kadar so bili zbrani ali obdelani v nasprotju z zakonom (‘pravica do ugovora’);
- **zavrniti** ali **privoliti** v obdelavo naših osebnih podatkov;

- **do pritožbe** pred neodvisnim organom za varstvo osebnih podatkov, če naših pravic ne spoštujejo; in
- zahtevati zaščito naših pravic pred **sodiščem**.

PRIMERI IZ RESNIČNEGA ŽIVLJENJA

Avstrijski študent, Max Schrems, se je leta 2007, med študijem prava s področja zasebnosti in varstva osebnih podatkov, odločil, da bo v praksi preveril svojo 'pravico do seznanitve' z lastnimi osebnimi podatki. Imel je svoj Facebook profil, zato je pisal družbi Facebook in jih zaprosil za kopijo vseh svojih osebnih podatkov, ki so jih hranili o njem. Glede na to, da je Max svoj profil uporabljal šele nekaj let in še to bolj poredko, je bil zelo presenečen, ko je v odgovor na svojo zahtevo prejel več kot 1.200 strani informacij o sebi. Toliko bolj presenečen je bil, ko je med prebiranjem informacij ugotovil, da je Facebook obdržal slike, za katere je mislil, da so bile izbrisane, prav tako pa je odkril ogromno ostalih podatkov, za katere je menil, da jih Facebook sploh ne bi smel hraniti. Max Schrems je takrat pričel z vseevropsko iniciativo, s katero je od Facebooka zahteval, naj začne spoštovati svoje obveznosti, med drugim tudi tako, da je proti družbi sprožil sodne postopke.

IDEJE ZA POGOVOR

1. **Razmislek o obravnavani temi.** Pravica do varstva osebnih podatkov pride v poštev kadarkoli nekdo o nas zbira osebne podatke, tudi če želi ta oseba ali organizacija podatke le pridobiti in shraniti, ne da bi jih nadalje uporabljala. Učence je treba spodbuditi, da razmislijo o tem, zakaj je tako: V čem je težava, če določena organizacija prične z obsežnim zbiranjem vseh mogočih podatkov o ogromnem številu ljudi? Ali otroci menijo, da bi moralo biti dovoljeno, da lahko organizacija zbira podatke o njih, ne da bi oni sami vedeli za to?

PRIPOROČENE DEJAVNOSTI

1. **Kako prepoznati osebne podatke.** Varstvo osebnih podatkov se razteza na vse osebne podatke. Kljub temu včasih ni enostavno ločiti med tem, kateri podatki so 'osebni podatki' in kateri ne. Nekateri podatki v nekem trenutku morda niso osebni podatki, lahko pa to postanejo kasneje. Za boljše razumevanje te problematike naj učenci **pogledajo sliko** nekoga, ki ima zakrit obraz ali se ga na sliki ne vidi dobro, in razpravljajo o tem, ali slika

predstavlja osebne podatke ali ne. Nato naj razmislijo o tem, kaj bi se zgodilo, če bi nekdo na spletu na tej sliki (sicer v obraz neprepoznavnega) posameznika označil z imenom in priimkom. Bi podoba posameznika, dogajanje na sliki ali lokacija takrat predstavljali njegove osebne podatke?

ZA NAJMLAJŠE

Najmlajši učenci naj se naučijo, da imajo, kadarkoli nekdo želi njihove osebne podatke, glede teh podatkov **določene pravice**.

ZA STAREJŠE IN/ALI BOLJ ZRELE

Starejši učenci naj se naučijo prepoznati, kaj so osebni podatki. Pridobijo naj jasen pregled nad svojimi **pravicami** v povezavi z osebnimi podatki: vedeti morajo, kdo razpolaga z njihovimi podatki in zakaj, kako dostopati do teh podatkov, kako zahtevati popravo svojih osebnih podatkov in, kadar je to primerno in ustrezno, kako zahtevati njihov izbris.

3. KDO ŽELI TVOJE OSEBNE PODATKE?

Zakaj je varstvo osebnih podatkov dandanes tako pomembno? Kdo želi pridobiti naše podatke in katere omejitve mora ob tem upoštevati?

CILJI

Poglavje je usmerjeno k temu, da učenci:

- dobijo predstavo o tem, zakaj organizacije pridobivajo, zbirajo, hranijo in uporabljajo naše osebne podatke;
- spoznajo dolžnosti, ki jih imajo organizacije, ko uporabljajo zbrane osebne podatke.

KLJUČNI POUČENI

Na dnevni ravni **vsak od nas ustvari ogromno količino podatkov**, predvsem **na spletu**, denimo, ko objavimo informacije, slike, videoposnetke ali ko te delimo z drugimi, ko preverjamo elektronsko pošto, prebiramo spletne novice, ali igramo igre na spletu – vse te dejavnosti ustvarijo podatke, ki jih je mogoče povezati z nami. Osebne podatke pa seveda ustvarjamo tudi, ko nismo na spletu, ko opravimo telefonski pogovor, med nakupovanjem in plačevanjem z bančno kartico, ko uporabimo javni prevoz in celo takrat, ko se zgolj sprehajamo in našo podobo ujame videonadzorna kamera. Veliko naših dejavnosti v vsakdanjem življenju ima tudi **spletno dimenzijo**: ko gremo v kino, na koncert ali na nogometno tekmo ter preko spleta kupimo vstopnice za dogodek, se o našem nakupu zabeležijo podatki, ki so naši osebni podatki.

Organizacije in podjetja osebne podatke zbirajo, hranijo in uporabljajo predvsem za to, da bi se s storitvami čim bolj približali našim specifičnim potrebam. Pogosto pri tem zasledujejo **pomemben cilj**, kot je na primer zagotavljanje otroškega varstva ali zdravstvene oskrbe.

Nekatere družbe pa želijo zbrati **kar največ podatkov** o ljudeh na splošno in še posebno o svojih strankah, in sicer za **namene trženja svojih storitev**. To jim omogoča, da prilagodijo svoje delovanje in povečajo število svojih strank ali da stranke pripravijo do tega, da za njihove storitve porabijo čim več denarja.

Osební podatki imajo zaradi tega veliko **gospodarsko vrednost**. Za veliko podjetij predstavljajo osebni podatki želeno dobrino in vir znatnih prihodkov; mnogo podjetij uporablja osebne podatke za oglaševanje in ustvarjanje ali povečevanje svojega dobička. Osebni podatki so lahko izjemno pomembni tudi za **državne organe**, saj z njimi dobijo boljši vpogled v življenje in delovanje posameznikov ali skupine posameznikov.

Nenadzorovana uporaba osebnih podatkov lahko pomeni prekomerno moč v rokah podjetij in državnih organov, zaradi katere posamezniki postanejo ranljivi.

Da bi preprečili zlorabo osebnih podatkov, pravo tistim, ki želijo podatke obdelovati, nalaga vrsto obveznosti. 'Upravljalci osebnih podatkov' imajo tako dolžnost:

- **pošteno** obdelovati osebne podatke;
- obdelovati osebne podatke samo za določene, **izrecne namene**;
- uporabiti le nujno potrebne osebne podatke (to pomeni, da uporabijo le tiste osebne podatke, ki so ustrezni, primerni in ne pretirani) in jih hraniti **le toliko časa, dokler je to potrebno za določen namen**;
- hraniti **točne, popolne in ažurne** osebne podatke in s tem zagotavljati njihovo ustreznost; ter
- zavarovati podatke, pri čemer morajo preprečiti dostop vsakomur, ki nima pravice, da bi do njih dostopal.

IDEJE ZA POGOVOR

1. **Kršitev varstva osebnih podatkov:** Učenci naj razmišljajo o tem, zakaj morajo imeti podjetja in organizacije, ki obdelujejo velike količine osebnih podatkov, določene dolžnosti v zvezi z varstvom osebnih podatkov. O obveznostih naj razmišljajo skozi primere kršitve varnosti podatkov, denimo kadar nepooblaščená oseba pridobi dostop do teh podatkov, čeprav ne bi smela. Predelajo naj naslednja vprašanja: So že slišali za kakšen primer 'kršitve varnosti osebnih podatkov' ali primer, ko je podjetje ali organizacija izgubila nadzor nad določenimi osebnimi podatki posameznikov? Bi bili zaskrbljeni, če bi nekdo, ki obdeluje njihove osebne podatke, utrpel napad spletnih hekerjev, ki bi te podatke ukradli? Katere 'kršitve varnosti podatkov' jih najbolj skrbijo in zakaj?
2. **Dobronamerni hekerji?** Kot nadaljevanje prejšnje teme naj učenci razmislijo o tem, da nekateri hekerji trdijo, da nezakonito dostopajo do podatkov samo

zato, da pokažejo, da podatki niso dobro zavarovani in tako želijo podjetja prisiliti, da jih močneje in bolj učinkovito zavarujejo. Učenci lahko razmislijo npr. o podjetju, ki izdeluje elektronske naprave za učence (kot npr. otroške fotoaparate ali tablične računalnike) in ga napadejo hekerji, da bi razkrili, da podjetje res slabo varuje podatke otrok. Ali imajo hekerji pravico do tega? Kakšna so tveganja pri njihovih aktivnostih? Ali obstajajo boljši načini za obravnavanje tega problema?

PRIPOROČENE DEJAVNOSTI

1. **Zveste stranke.** Veliko trgovcev in prodajnih verig spodbuja svoje stranke, naj pridobijo njihove kartice zvestobe, ki jih morajo predložiti vsakič, ko opravijo nakup. S to vajo v razredu spodbudimo razpravo o klubih zvestobe in o obdelavi osebnih podatkov, ki jih podjetja s pomočjo kartic zvestobe pridobijo o kupcih:
 - Učenci naj najprej **govorijo o** svojem dožemanju kartic zvestobe: So takšne kartice za stranke uporabne? So koristne za podjetja? Kakšne vrste podatkov zbirajo podjetja s pomočjo kartic zvestobe?
 - Vsak učenec naj **izbere** kartico zvestobe, ki jo uporablja on ali njegova družina, pri čemer naj na kratko opredeli: 1) informacije, ki jih je treba posredovati podjetju za pridobitev kartice; 2) informacije, ki jih podjetje zbere, ko uporabijo kartico in 3) namen, za katerega podjetje te podatke zbira. Za to vajo bodo učenci morda morali preveriti spletno stran podjetij, njihove brošure ali podjetja neposredno zaprositi za odgovore.
 - Če so v razredu učenci, katerih družine ne uporabljajo kartic zvestobe, lahko, **kot alternativo**, opišejo informacije, ki jih trgovci med nakupovanjem zbirajo o njih. Na primer, če nakupujejo preko spleta, ali trgovci shranijo informacije o njihovih nakupih?
 - **Delite in primerjajte** rezultate vsake posamezne ugotovitve.
 - **Razpravljajte** o tem, kakšno prednost pridobi podjetje z zbiranjem osebnih podatkov svojih strank.
 - Za konec naj učenci **razmislijo** še o tem, kaj so se naučili: So se zavedali, katere podatke trgovci zbirajo in obdelujejo o njih in njihovi družini? Ali menijo, da se ljudje na splošno zavedajo, kaj se dogaja z njihovimi osebnimi podatki? Bi bilo za ljudi koristno, če bi bili o tem bolje obveščeni?

ZA NAJMLAJŠE

Najmlajši učenci naj se naučijo, da so njihovi podatki **dragoceni**, da lahko ljudje zbirajo njihove podatke le, če imajo za to dober razlog in da lahko to počnejo le zelo previdno in na varen način.

ZA STAREJŠE IN/ALI BOLJ ZRELE

Starejši učenci naj bodo seznanjeni s tem, da dnevno ustvarimo **veliko količino** podatkov in da so **različna podjetja in organizacije** zelo zainteresirane za uporabo teh podatkov za različne namene. Naučijo naj se tudi, da ko nekdo obdeluje osebne podatke, mora ob tem spoštovati določena **pravila**, ki so postavljena zato, da nas varujejo pred zlorabami.

4. ODLOČI SE PAMETNO IN PUSTI DRUGIM, DA SE ODLOČIJO SAMI

Vsakdo se ima pravico odločiti, ali bo dovolil, da nekdo drug pridobi ali uporablja njegove osebne podatke. To pomeni, da morajo drugi upoštevati naše želje glede tega, kaj želimo ali dovolimo, da se zgodi z našimi osebnimi podatki. Tudi sami pa moramo ravnati enako, ko se srečamo z osebnimi podatki drugih ljudi – pustiti jim moramo, da o svojih podatkih odločijo sami.

CILJI

To poglavje bo učencem pomagalo pri:

- učenju o možnosti **privolitve** ali zavrnitve glede zbiranja naših osebnih podatkov;
- krepitevi zavedanja, da je privolitev mogoče **preklicati**;
- razumevanju, da morajo včasih tudi otroci **vprašati druge za njihovo privolitev**, preden na spletu delijo določeno vsebino.

KLJUČNI POUČENI

Včasih smo **dolžni** posredovati nekatere osebne podatke drugim. Če na primer želimo naročiti dostavo pice, moramo piceriji posredovati svoj naslov, sicer ne bodo vedeli, kam naj nam pico dostavijo.

V drugih primerih pa bodo nekatera podjetja želela pridobiti **več podatkov, kot je to nujno potrebno**. Morda bodo želela pridobiti več informacij o svojih strankah in uporabnikih svojih storitev kot na primer njihovo starost, spol, najljubši hobi. Te podatke sicer lahko zahtevajo, vendar morajo hkrati povedati, kaj bodo z njimi počeli in dati posamezniku možnost, da v posredovanje podatkov **privoli** ali da posredovanje podatkov **zavrne**.

Da bi bila privolitev veljavna, mora biti **prostovoljna, izrecna, informirana in nedvoumna**. To pomeni, da:

- nas v 'privolitev' za posredovanje podatkov nihče ne sme prisiliti;
- lahko privolimo le v izrecno navedeno uporabo podatkov in ne v uporabo podatkov na splošno, recimo za kakršenkoli namen, ki si ga bodo drugi zamislili;

- nas lahko vprašajo za privolitev le, če nam podajo podrobne informacije o tem, v kaj bomo privolili; in
- je naša privolitevupoštevna le, če je bila izražena izrecno in nedvoumno.

Preden se posameznik odloči, ali bo v posredovanje svojih osebnih podatkov privolil, ali bo to zavrnil, naj si vzame čas za razumevanje tega, **kateri podatki** bodo o njem zbrani, **za kakšen namen**, kdo bo **odgovoren** za njihovo zavarovanje in **kako jih lahko obvesti**, če si premisli glede svoje privolitve in zahteva, da se podatki izbrišejo. Če posamezniku navedene okoliščine niso povsem razumljive ali če se z njimi ne strinja, lahko posredovanje svojih osebnih podatkov **zavrne**.

Otrokom je včasih težko razumeti posledice privolitve v posredovanje svojih osebnih podatkov, zato **ti ne morejo veljavno privoliti** v posredovanje podatkov, preden dosežejo določeno starost ali zrelost. V Sloveniji je starostna meja, pri kateri lahko otrok sam poda veljavno privolitev v tako obdelavo osebnih podatkov, ki ne posega bistveno v njegovo življenje v prihodnosti, trenutno 15 let. Podjetja oz. organizacije, ki želijo pridobiti osebne podatke otrok mlajših od te starosti, morajo za privolitev **vprašati njihove starše oz. skrbnike**, ki lahko v posredovanje podatkov privolijo, ali privolitev odklonijo. Kljub temu da otroci niso vedno sposobni sami privoliti ali privolitev zavrniti, pa morajo starši oziroma skrbniki otrokova stališča upoštevati v največji možni meri. Otroci imajo namreč pravico **izraziti svoja stališča** v vseh stvareh, ki jih zadevajo.

Tudi tisti posamezniki, ki so privolili v posredovanje svojih osebnih podatkov, imajo vedno pravico, **da si premislijo**. To je še posebej pomembno pri podatkih o kraju, kjer se posameznik nahaja, pri t. i. **lokacijskih podatkih**. Posameznik je namreč lahko privolil v to, da je aplikacija na mobilnem telefonu med iskanjem poti pridobila njegove lokacijske podatke, vendar ne želi, da bi ta aplikacija tudi kasneje spremljala vsak njegov korak. Ker je do tega upravičen, ima posameznik pravico, da svoje soglasje prekliče. Naprave, ki zbirajo lokacijske podatke, morajo na to redno opozarjati uporabnike: ti lahko namreč pozabijo, da so privolili v zbiranje lokacijskih podatkov, ali pa je to privolitev dala kakšna druga oseba, ki je uporabljala isto napravo.

Vsakdo, ki je sposoben dati privolitev, ima privolitev pravico tudi preklicati. Če so za otroka dali privolitev starši, lahko otrok takšno privolitev staršev prekliče, ko doseže 'privolitveno starost', če se tako odloči.

Ne nazadnje pa se moremo zavedati tudi, da kadar drugih ljudi ne vprašamo, ali dovolijo, da posredujemo ali objavimo njihove osebne podatke, sami lahko **posežemo v njihove pravice**. Kadar želimo na spletu objaviti fotografijo z drugimi osebami, jih moramo torej prositi za njihovo soglasje. Vprašati jih moramo, ali se z objavo strinjajo, prav tako pa moramo **spoštovati njihovo odločitev**, če se odločijo, da objave ne želijo. Če je oseba mladoletna, moramo za privolitev vprašati njihove starše ali skrbnike.

IDEJE ZA POGOVOR

1. ***Svobodna privolitev:*** Načeloma lahko svobodno 'privolimo' v obdelavo svojih osebnih podatkov le takrat, ko lahko tako obdelavo svobodno tudi zavrremo. Včasih pa so tisti, ki od nas zahtevajo privolitev, v posebnem položaju (na primer, ker so zelo priljubljeni), zaradi česar je obdelavo osebnih podatkov težko zares svobodno zavrniti. Učenci naj razmislijo o tem, ali se počutijo resnično 'svobodne' pri uporabi ali prenehanju uporabe spletnih storitev in aplikacij, ki jih redno uporabljajo in ki o njih zbirajo osebne podatke, kot so na primer različna družbena omrežja. Ob tem naj otroci razmišljajo o naslednjem: Zakaj dejansko uporabljajo te storitve in ne katerih drugih? Je to morda zaradi tega, ker jih uporablja večina prijateljev, ki jih poznajo? Se počutijo pod pritiskom, da jih morajo zaradi tega uporabljati tudi sami?

PRIPOROČENE DEJAVNOSTI

1. ***Pogoji uporabe:*** Ta vaja je namenjena tistim učencem, ki so že dovolj stari ali zreli, da lahko privolijo v obdelavo svojih osebnih podatkov. Cilj vaje je prikazati, da si pred 'privolitvijo' včasih ne vzamemo dovolj časa, da bi se ustrezno poučili o tem, v kaj bomo privolili.
 - Učenci naj najprej **napišejo ime** aplikacije ali spletne storitve, ki jo posebej pogosto uporabljajo in ki zbira njihove osebne podatke. Priporočeno je, da ne izberejo vsi iste storitve, temveč skupaj izberejo vsaj nekaj različnih.
 - Učenci naj nato napišejo **vse, kar so si zapomnili** iz 'pogojev uporabe' ali 'politik zasebnosti' posamezne storitve, ki naj bi posameznikom pojasnila, kaj podjetje počne z njihovimi podatki in s katero so se morali strinjati, preden so se v aplikacijo registrirali. Tudi v primeru, če se ne spomnijo vsebine pogojev uporabe in politik zasebnosti, naj se poskušajo spomniti vsaj, kje so se srečali s temi pogoji.

- Po tem, ko bodo svoje odgovore zbrali in zapisali, naj jih primerjajo z dejanskimi 'pogoji uporabe' oz. 'politikami zasebnosti', in sicer tako, da jih preverijo v aplikaciji oz. storitvi.
- Na koncu te naloge naj se učenci pogovorijo o tem, kaj so se naučili iz te izkušnje: Ali učenci vedo, kaj jim podjetja sporočajo? So si kadarkoli vzeli čas in prebrali pogoje uporabe in politike zasebnosti? Če da, ali menijo, da so napisane na uporabniku prijazen način?

ZA NAJMLAJŠE

Najmlajši učenci morajo vedeti, da **ne smejo nikoli posredovati svojih osebnih podatkov** brez soglasja svojih staršev. Prav tako morajo razumeti, da ne smejo nikoli objavljati podatkov o drugih ljudeh (vključno s slikami in videoposnetki), ne da bi jih prej vprašali za soglasje.

ZA STAREJŠE IN/ALI BOLJ ZRELE

Starejši učenci morajo pridobiti **veščine, potrebne za to, da lahko podajo ustrezno privolitev (ali zavrnitev)**: ko so soočeni s situacijo, da nekdo od njih zahteva osebne podatke, se morajo prepričati, da razumejo, za kakšen namen oseba potrebuje te podatke, katere podatke potrebuje, kdo jih bo hranil in kako lahko z njo stopi v stik, če bi želel več informacij ali če si glede odločitve premisli. Učenci morajo razumeti, da lahko vedno rečejo ne in da lahko glede česar koli, kar niso razumeli, postavijo dodatna vprašanja. Prav tako morajo razumeti, da morajo tudi sami pred **uporabo osebnih podatkov drugih oseb te prositi za soglasje** in spoštovati njihovo odločitev.

5. SPLETNA IDENTITETA

Kako odraščati s spletno identiteto? Naši podatki, ki se nahajajo na spletu, imajo lahko resne posledice za naše življenje, zato je pomembno, da se vprašamo, katere podatke naj bi delili o sebi, kdaj in pod kakšnimi pogoji.

CILJI

To poglavje bo učencem pomagalo:

- postati bolj ozaveščeni o svoji prisotnosti na spletu in pridobiti bolj kritičen odnos do razkrivanja svojih podatkov na spletu;
- razmisliti o pomenu posameznikove **spletne identitete**;
- razmisliti o tem, kako lahko nadzorujejo svoje digitalne odtise, ki jih puščajo na spletu.

KLJUČNI POUČENKI

Zbir vseh informacij, ki jih je o posamezniku mogoče pridobiti na spletu, imenujemo '**spletna identiteta**' oziroma posameznikova 'prisotnost na spletu'. Zgolj s poznavanjem našega imena si lahko druge osebe, ki nas sicer ne poznajo, o nas ustvarijo vtis ali začetno mnenje. Spletno identiteto lahko razumemo kot element naše '**identitete**', ki ima več različnih razsežnosti: v očeh babice nismo enaki kot v očeh najboljšega prijatelja, naše obnašanje se razlikuje, kadar smo v svoji sobi ali kadar nakupujemo v trgovini, prav tako nas morda sošolci dojemajo drugače kot vrstniki, ki smo jih srečali med poletnimi počitnicami.

Ljudje čedalje več uporabljamo internet, zato so postale naše '**spletne identitete**' in naš '**spletni ugled**' zelo pomembni. Kadar nekdo išče službo ali se želi prijavit za štipendijo, lahko delodajalci oz. institucije za štipendiranje že s kratkim pregledom spleta pridobijo veliko dodatnih informacij o kandidatu. Če jim te informacije niso všeč, lahko kandidata enostavno ne zaposlijo oz. mu ne podelijo štipendije. Tudi v zasebnem življenju se pogosto dogaja, da spoznamo nekoga, za katerega bi si želeli, da postane naš prijatelj ali partner, ta oseba pa bo o nas na spletu poiskala dodatne informacije. Informacije na spletu nam lahko pogosto škodijo, nas spravijo v zadrego ali v neprijeten položaj.

Naša 'spletna identiteta' ni nikoli povsem enaka naši dejanski identiteti. V določenih primerih je naša 'spletna identiteta' še posebej **zavajajoča**, in lahko v

ljudeh pusti vtis, da smo storili kaj, česar v resnici nismo, ali ljudi spominja na dogodke, ki jih sami štejemo za stvar preteklosti ali bi jih radi pozabili.

V Evropi je zaradi tega sedaj priznana tudi '**pravica do pozabe**', s katero lahko posameznik pri spletnih iskalnikih zahteva, da umaknejo povezave do rezultatov iskanja, ki so **neprimerni ali nepopolni**. Sam obstoj te pravice dokazuje, da imajo rezultati, ki jih posamezniki najdejo o nas med spletnim brskanjem, dejanske posledice tudi za naše resnično življenje.

Vseeno pa ta pravica ne pomeni, da lahko kadarkoli zahtevamo izbris svojih osebnih podatkov s spleta. Celotako, ko imamo pravico zahtevati izbris določenih podatkov, **to v praksi ni tako enostavno**. Lahko se celo zgodi, da so si posamezniki, ne glede na izbris s spleta, vsebino že shranili na svoje računalnike ali druge naprave in jo ponovno delili z drugimi.

Zato je resnično najbolje, da **dvakrat premislimo**, preden karkoli objavimo na spletu. Mladostniki se morajo zavedati, da so vsi podatki o njih kot 'digitalne drobtinice' ali '**spletni odtisi**,' ki bodo nekega dne **vodili do njih** in ki jih je **zelo težko izbrisati**. Nekatere je celo tako težko izbrisati, da je o njih boljše razmišljati kot o '**digitalnih tatujih**,' ki nas bodo spremljali vse življenje.

PRIMERI IZ RESNIČNEGA ŽIVLJENJA

- Nekega Španca so zalotili pri uriniranju v javnosti in mu zaradi tega izrekli globo. Špansko pravo določa, da policija tak prekršek objavi v uradnem glasilu na spletu, če ne pozna naslova, kamor bi poslala položnico za plačilo globe. Španec se je kasneje zaposlil kot ravnatelj na šoli. Učenec te šole je z uporabo spletnega brskalnika odkril izrečeno kazen in to informacijo delil s preostalimi učenci. To je resno vplivalo na ravnateljev ugled med učenci, zaradi česar je bilo njegovo delo zelo oteženo.
- Med uro zgodovine na fakulteti je madžarski študent posnel nekaj fotografij, na katerih je bilo jasno razviden njegov obraz in razni nacistični simboli. Nekdo je slike objavil na spletu, nato pa so se avtomatično prikazale med rezultati iskanja, kadar so ljudje v spletni iskalnik vpisali ime študenta. Ker je študenta skrbelo, da bi to lahko vplivalo na njegove možnosti zaposlitve, je zaprosil ponudnike spletnih iskalnikov, da njegovega imena ne povezujejo več z navedenimi slikami. S pomočjo organov za varstvo osebnih podatkov mu je to tudi uspelo.

NASVETI

Se na spletu nahajajo vaši podatki, ki bi jih želeli izbrisati?

- Najprej se obrnite na osebo, ki je podatke objavila, in jo prosite, da podatke izbriše.
- Če ste podatke objavili sami, jih lahko poskusite tudi izbrisati sami. Vse spletne storitve naj bi posameznikom omogočale, da izbrišejo svoj profil ali uporabniški račun, če tako želi.
- Če zgornji koraki ne vodijo do uspeha, kontaktirajte osebo ali podjetje, ki ima v lasti spletno stran oz. platformo, na kateri so podatki objavljeni.
- Če ne deluje nič od navedenega, prosite za pomoč osebo z več znanja, ki ji zaupate. Za pomoč se lahko obrnete tudi na organe, ki skrbijo za varstvo osebnih podatkov.

IDEJE ZA POGOVOR

1. **Zakaj je moj spletni ugled sploh pomemben?** Učenci naj razmislijo o tem, kdaj in zakaj so njihove spletne identitete pomembne. To lahko storijo predvsem tako, da:
 - Razmislijo o **tipičnih situacijah**, v katerih ljudje navadno po spletu iščejo podatke o drugih osebah. Taki primeri so lahko povezani z delom (Ali bi po spletu preverili osebo, preden bi ji ponudili zaposlitev v svojem podjetju?); sobivanjem (Bi po spletu preverili osebo, preden bi z njo delili stanovanje?); družbenimi odnosi (Ali obstaja verjetnost, da vas bodo osebe, ki jih boste spoznali v prihodnosti, preverile po spletu?) ipd.
 - Razmislijo o **posebnih skupinah ljudi**, za katere bi lahko bil spletni ugled zelo pomemben. Učenci naj razmislijo o tem, kaj bi se zgodilo, če bi se kdo izmed njih kdaj začel ukvarjati s politiko, postal slavni igralec ali vrhunski športnik? Ali bi ostale ljudi zanimale informacije, ki jih je mogoče dobiti po spletu? Bi si morda takrat želeli, da nekaterih podatkov ali slik ne bi bilo na spletu?
2. **Kaj se vam zdi, da resnično ne sodi na splet?** Učenci naj premislijo o tem, katere vsebine so posebno problematične, če so prosto dostopne na spletu. Pri tem lahko razmišljajo o svojih osebnih izkušnjah in se skušajo spomniti, ali so že kdaj videli ali prebrali kakšno informacijo, zaradi katere so si o določeni osebi izoblikovali slabo mnenje. Razmislijo lahko na primer:
 - O podatkih, ki so lahko **preveč intimni za objavo**: Ali obstajajo vsebine, za katere je pametneje, če jih nikoli ne bi objavili na spletu? Katere in zakaj?
 - O podatkih, ki jih je mogoče **razumeti narobe**: Ali obstajajo podatki, ki jih je mogoče na enostaven način vzeti iz konteksta? Ali obstajajo nejasne in dvoumne fotografije, ki lahko vodijo do napačnih interpretacij? Obstajajo spletni profili, na katerih si je moč ustvariti le delno predstavo o osebi?
 - O podatkih, ki lahko **hitro postanejo nepopularni**: Ali obstajajo vsebine, ki so danes zanimive, že jutri pa so lahko povsem iz mode? Vas je bilo kdaj sram zaradi dejanj, ki ste jih storili pred več leti?

PRIPOROČENE DEJAVNOSTI

1. Učenci naj z uporabo spleta **raziščejo, kateri podatki o njih so na voljo javnosti**. V nekaterih primerih lahko to vodi do nepričakovanih odkritij. Otroci lahko odkrijejo, da so informacije, za katere so mislili, da so zaupne,

dostopne širši javnosti ali da so informacije, ki naj bi bile dostopne le njihovim (spletnim) prijateljem, dostopne vsakomur. Da bi preprečili morebitne neprijetne situacije, naj učenci to nalogo opravijo sami, najbolje doma.

- Kasneje se lahko v razredu pogovorite o tem, kaj so se naučili, ali pa učenci o tem napišejo spis.
- še ena od možnih nalog pa je, da učenci preverijo, ali lahko na spletu najdejo osebo, ki ima enako ime kot oni sami. Nekatero od najdenih primerov lahko izberete, nato pa naj učenci v manjših skupinah poskusijo najti vse javno dostopne informacije o osebi z istim imenom. Vsaka skupina lahko nato pripravi predstavitev te osebe, kakor si jo predstavljajo glede na zbrane podatke. Po opravljeni nalogi se lahko pogovorite o naslednjih vprašanjih: Ali lahko pridobimo zelo podrobno predstavo o osebi zgolj s spletnim iskanjem? Kaj bi se lahko zgodilo, če bi kdo iskal informacije o učencu, ki ima enako ime kot nekdo drug?

ZA NAJMLAJŠE

Najmlajši učenci naj se naučijo, da si ljudje podatke, ki so na spletu, lahko razlagajo po svoje in da drobci informacij, ki jih splet vsebuje o nas, dajo ljudem določeno predstavo o tem, kakšni smo. Zaradi tega moramo vsi dvakrat premisliti, preden na spletu karkoli objavimo.

ZA STAREJŠE IN/ALI BOLJ ZRELE

Starejši učenci morajo razumeti, da imajo lahko spletne informacije hude posledice za naša življenja, zato si zaslužijo vso potrebno skrb. Glavno vodilo naj bo, da učenci na spletu ne delijo tistih informacij, ki jih ne bi želeli deliti s širšo javnostjo, denimo v gledališču.

6. SPLETNO OGLAŠEVANJE

'Biti povezan' ne pomeni samo aktivno objavljati in deliti informacij, ki jih sami izberemo. Kadarkoli namreč uporabljamo elektronske naprave, lahko te ustvarjajo in drugim posredujejo podatke o nas in o tem, kaj počnemo. Ti podatki so še posebej dragoceni za podjetja, ki prodajajo oglaševalski prostor, zato pogosto zbirajo naše podatke s ponujanjem 'brezplačnih' storitev.

CILJI

To poglavje bo učencem pomagalo pri:

- spoznanju, da so njihove spletne aktivnosti pogosto pod nadzorom;
- razumevanju, da jim podjetja ponujajo oglase in izdelke na podlagi njihovega predhodnega obnašanja na spletu.

KLJUČNI POUČENI

Kadarkoli uporabljamo računalnik, pametni telefon, tablico, igralno konzolo ali katerokoli drugo napravo za komuniciranje ali napravo, ki se lahko poveže na splet, **ustvarjamo podatke**. Nekateri od teh podatkov **povedo, kaj počnemo**: to so spletne strani, ki smo jih obiskali, videoposnetki, ki smo si jih ogledali, igre, ki smo jih igrali, osebe, s katerimi smo izmenjali sporočila, besede, ki smo jih vtiskali v spletni iskalnik, in mnogi drugi podatki. Nekateri podatki **povedo, kje smo**: ti podatki nas lahko locirajo na zemljevidu ali nas na primer povežejo s krajevno različico spletne strani. Nekateri podatki pa so **podatki o nas** (naša telefonska številka, naslov elektronske pošte, vsi podatki, ki nas ločijo od drugih oseb). Vsi ti podatki omogočajo podjetjem, da si ustvarijo zelo natančno sliko o tem, **kdo smo**, kakšno življenje živimo, **kaj imamo radi** in **za kaj radi trošimo denar**. Zelo verjetno je, da imajo podjetja precej natančen uvid v to, koliko denarja pravzaprav sploh imamo. Podjetja in druge organizacije uporabljajo vse te informacije za to, da ljudi **'profilirajo'** in jih razvrščajo v različne kategorije.

Dejstvo je, da se ne **zavedamo** vedno, v katere zbirke se zabeležijo naši osebni podatki, kljub temu, da bi nam moral vsak, ki zbira naše podatke, to jasno povedati. Ljudje čedalje bolj in kot po tekočem traku sprejemamo **'pravila uporabe'** pred uporabo posamezne spletne storitve ali pred namestitvijo določene aplikacije, ne da bi jih sploh prebrali. Tudi ko jih preberemo, nam ta pogosto sploh niso razumljiva, kar še toliko bolj velja za mlajše osebe.

Podobno velja tudi za spletne strani, ki za zbiranje osebnih podatkov uporabljajo 'piškotke'. Spletne strani so dolžne obvestiti svoje uporabnike o tem, katere njihove podatke zbirajo in za kakšne namene ter jim ponuditi možnost, da uporabo določenih piškotkov sprejmejo ali odklonijo. Kljub temu pa večina ljudi nima časa, da bi razmišljala o piškotkih na vsaki spletni strani, ali ima težave z razumevanjem, zakaj je takšno zbiranje podatkov sploh problematično.

Večina spletnih strani svoje obiskovalce profilira na podlagi njihovega spletnega obnašanja z namenom, da **proda svoj oglaševalski prostor**. Če spletno stran pogosto obiskujejo otroci, bo svoj oglaševalski prostor poskušala prodati podjetjem, ki prodajajo igrače. Podjetja so celo sposobna **prilagoditi vsak posamezni oglas temu, kar zanima posameznega obiskovalca strani**. Ko bodo denimo otroci, ki imajo radi sestavljanke, obiskali določeno spletno strani, jim bo ta spletna stran lahko ponudila oglas za sestavljanke.

Takšnim praksam pravimo 'vedénjsko' oz. 'ciljno oglaševanje'. Mladoletniki se morajo zavedati, da je prikazana vsebina na spletnih straneh včasih namenjena izključno njim in da je do tega prišlo na podlagi njihovega predhodnega vedénja. Rezultati spletnega brskanja so deloma rezultat tega, kar splet 've o nas', velikokrat pa izpostavljajo tudi izdelke, ki jim posebno pozornost namenjajo spletne trgovine.

Otroci morajo razumeti, da podjetja, ki svoje storitve ponujajo 'brezplačno', to počnejo zato, ker **zaslužijo denar** s prodajanjem podatkov o nas, ki so jih pridobili, ko smo brezplačno uporabljali njihove storitve. Več ljudi kot bodo take storitve privabile, več denarja bodo ponudniki zaslužili; zaradi tega se jim 'brezplačno' ponujanje storitev pravzaprav zelo izplača.

IDEJE ZA POGOVOR

1. **Ali plišasti medvedki vohunijo za otroki?** Nekatera podjetja, tudi takšna, ki prodajajo otroške igrače, razvijajo t. i. 'pametne igrače'. Te igrače omogočajo interakcijo z otroki in pošiljajo podjetju informacije o njih. Te informacije so v osnovi sicer namenjene temu, da je odziv igrače bolj realističen in zanimiv, seveda pa omogočajo podjetjem tudi zbiranje podatkov o otrocih. Učenci naj premislijo o tem, ali jim je všeč, da imajo plišasti medvedki in lutke vgrajene kamere in mikrofone, ki lahko posnamejo zvok in sliko, posnetke pa nato posredujejo podjetju. Bi si tudi sami želeli kupiti tako igračo? Če da, ali menijo, da bi morali imeti možnost, da take funkcije izklopijo? Kaj pa, če bi

igračo pozabili izklopiti, ta pa bi zabeležila podatke, za katere ne bi želeli, da jih kdorkoli izve?

2. **Enake možnosti?** Kadar smo na spletu, so nekatere prikazane informacije odvisne od tega, kaj podjetja mislijo, da nas zanima ali da bi želeli kupiti. Zaključki podjetij o tem, kaj nas zanima, pa temeljijo na podatkih, ki so jih zbrali o nas, oziroma celo od njihove interpretacije teh podatkov. To pomeni, da bodo učenci istega razreda videli različne oglase, ko bodo obiskali isto spletno stran. Včasih vsebina oglasov ne bo imela bistvenega vpliva na vsakdanje življenje – nekateri učenci bodo videli eno vrsto oblačil, drugi pa drugo vrsto. Lahko pa se zgodi, da so razlike večjega pomena. Morda nekateri učenci vidijo oglase za potovanja, ki jih drugi ne morejo videti, oglase za različne šole ali univerzitetne programe, oglase o različnih možnostih štipendiranja ali celo o različnih ponudbah za delo. Učenci naj razmislijo o tem, ali se jim tako razlikovanje zdi pošteno in naj pomislijo na primere, ko bi to lahko predstavljalo težavo. Razmislijo lahko tudi o možnih načinih, kako se s tem spoprijeti.

PRIPOROČENE DEJAVNOSTI

1. **Anonimne informacije.** Naslednja vaja spodbuja razmišljanje o informacijah, ki jih je mogoče izpeljati in pridobiti iz naših spletnih aktivnosti in preferenc.
 - Vsak učenec naj si določi **izmišljeno ime**, s katerim bo skrnil svojo pravo identiteto. Pod tem imenom naj na list papirja zapiše in izpolni **rubrike**, ki jih bo učitelj, upošteva starost otrok v razredu, predhodno določil. Te so lahko: najljubši tv programi, najljubša oblačila, najljubši šport, poznavanje različnih jezikov, najljubša glasba, zadnji film, ki so si ga ogledali, zadnja prebrana knjiga ipd. V tej fazi učitelj še ne sme razložiti namena te igre.
 - Vse liste papirja naj učenci nato premešajo. Učitelj naj izbere naključen list papirja in naglas prebere njegovo vsebino. Avtor besedila se mora po najboljših močeh potruditi, da ne razkrije svoje identitete, drugi učenci pa naj poskušajo **uganiti**, kdo je avtor besedila. Ali jim to lahko uspe že na podlagi ene informacije? Morda na podlagi dveh? Treh?
 - Kasneje, ali če nihče ni uganil, kdo je avtor, naj vsi učenci poskusijo premisliti, **koga bi zanimali** podatki osebe s takšnim profilom. Ali bi ti podatki lahko imeli gospodarsko vrednost tudi za nekoga, ki ne ve, kdo je avtor?

- Vajo je mogoče **ponoviti** večkrat in pri tem izbrati različne načine profiliranja.
- Starejši učenci lahko razmišljajo tudi o tem, kako lahko podjetja na spletu dobijo informacije, ki so jih zapisali na liste papirja. Kdo hrani podatke o tem, kar smo na spletu iskali? Katere spletne strani ponujajo možnost, da izrazimo, kaj nam je 'všeč'? Kdo hrani informacije o izdelkih, ki smo jih pregledovali? Kdo hrani informacije o videoposnetkih, ki si jih radi pogledamo?

ZA NAJMLAJŠE

Najmlajšim otrokom je treba predstaviti, da obstaja veliko elektronskih naprav, ki jih uporabljajo (ali ki jih bodo verjetno kmalu začeli uporabljati), ki so povezane v splet in **zbirajo podatke o njihovih življenjih**. To so lahko pametni telefoni, računalniki, tablice, igralne konzole ipd. Z uporabo teh naprav poskušajo podjetja pridobiti čim več informacij o tem, kaj radi počnemo, vse z namenom, da nam lahko prodajo čim več svojih izdelkov in storitev.

ZA STAREJŠE IN/ALI BOLJ ZRELE

Starejši učenci naj se naučijo, kako lahko različne naprave, ki jih uporabljajo, sledijo njihovim aktivnostim na spletu. Razumeti morajo tudi, da določene informacije, ki jih vidijo na spletu, kot denimo oglasi, morda niso povsem enaki tistim, ki jih vidijo drugi.

7. KAKO OHRANITI SKRIVNOSTI RES SKRITE?

Skrb za varstvo naših podatkov se začne z nami. Za to, da bi bili naši podatki na varnem, moramo biti previdni in sprejeti nekaj osnovnih tehničnih previdnostnih ukrepov.

CILJI

To poglavje bo učencem omogočilo, da:

- se zavejo nevarnosti, ki lahko ogrozijo njihove podatke;
- se naučijo, kako bolje zaščititi svoje podatke;
- spoznajo 'nastavitve zasebnosti';
- postanejo pozorni na 'krajo identitete' in 'ribarjenje podatkov'.

KLJUČNI POUČENKI

Svoje **digitalne podatke** hranimo na različnih mestih. Nekateri so shranjeni na fizičnih napravah, ki jih imamo pri sebi, kot na primer na računalnikih, tablicah ali pametnih telefonih. Nekatero druge podatke pa hranijo druge osebe in lahko do njih dostopamo tako, da se vpišemo v svoj račun ali profil. Pomembno je, da z ustreznimi ukrepi zagotovimo, da so **naši podatki varni**.

Poskrbeti moramo, da svoje naprave zaščitimo, npr. z zaklepanjem in določitvijo gesel, kar bo preprečilo ljudem dostop do naših naprav in podatkov. Zaščititi moramo tudi svoje spletne profile in račune. Glede na to, da do njih praviloma dostopamo z geslom, je ključnega pomena, da so **gesla varna** in jih poznamo **izključno mi**.

Varna hramba gesel za zasebne račune in profile pomeni, da jih moramo zadržati **strogo in izključno zase** in da jih **ne delimo z nikomer** niti z najboljšim prijateljem ali ljubeznijo svojega življenja. Skrb za varnost naših gesel je **naša odgovornost**, naša skrivnost, ki je ne smemo deliti z nikomer.

Učenci se morajo zavedati, da če jih nekdo prosi za njihovo zasebno geslo kot dokaz resničnega prijateljstva ali ljubezni, mu/ji ga ne smejo povedati. To bi namreč lahko ogrozilo njihove podatke in podatke vseh njihovih stikov. Oseba, ki sprašuje za geslo, bi v resnici morala kot dokaz svojega prijateljstva in ljubezni v celoti spoštovati njihovo zasebnost in **prenehati s takšnimi predlogi**.

Na spletu moramo imeti vedno pod nadzorom, kaj se dogaja z našimi podatki. To lahko učinkovito storimo tako, da pri vsaki storitvi, ki jo uporabljamo, preučimo '**nastavitve zasebnosti**'. Nastavitve zasebnosti so mehanizmi, ki omogočajo uporabnikom storitve, da se vsaj do določene mere lahko odločijo, kdo bo videl njihove informacije in vsebine na spletnem profilu.

'Nastavitve zasebnosti' bi morale uporabnikom pomagati pri nadzoru njihovih podatkov, a vendar jih **ni vedno enostavno** uporabljati. Včasih obstaja več različnih nastavitvev, s katerimi upravljamo informacije v profilu, sprejemamo odločitve o tem, kaj se bo zgodilo z objavami in se odločamo, kdo lahko vidi komentarje na sporočila drugih oseb ipd.

Pomembno je, da mladoletniki pri uporabi spletnih storitev:

- ne delijo javno informacij, kot so njihov naslov, telefonska številka ali elektronska pošta;
- se dobro zavedajo, katere objavljene informacije bodo dostopne vsem in katere le določenim ljudem ter katerim;
- vedo, katere informacije o njih lahko pridobijo drugi ljudje, ko vpišejo v iskalnik njihovo ime ali vzdevek.

Pri skrbi za varnost svojih podatkov moramo biti pozorni tudi na to, kako uporabljamo svojo elektronsko pošto. Nekatera sporočila, ki jih prejmemo, namreč lahko predstavljajo **prevaro** ali goljufijo. Na elektronski naslov lahko prejmemo sporočilo, da smo zadeli nagrado ali podedovali bogastvo od nekoga, za kogar nismo še nikoli slišali. Da bi prišli do izmišljene nagrade ali neobstoječega denarja, osebe od nas zahtevajo določene osebne podatke. A te podatke bodo nepridipravi uporabili zgolj za to, da bodo od nas pridobili denar ali kakšno drugo korist.

Posebej nevarna praksa je '**ribarjenje podatkov**' ali *phishing*. Pri tem uporabnik prejme sporočilo na videz zaupanja vrednega podjetja, ki želi pridobiti dostop do **osebnih podatkov** posameznika. Sporočila na prvi pogled izgledajo tako, kot bi jih poslala banka, ponudnik elektronskega naslova, ali družba, ki ponuja nakup spletnih iger ali aplikacij, a v resnici ni tako. Pošiljatelj nam sporoči, da za izvajanje storitve nujno potrebuje naše geslo ali druge podatke kot npr. datum rojstva, telefonsko številko ali naslov. Te podatke nato uporabijo za pridobivanje dostopa do naših spletnih računov, in sicer kot bi to storili v našem imenu, saj razpolagajo z našimi osebnimi podatki. Temu pravimo tudi '**kraja identitete**'.

Zgolj z nekaj pridobljenimi osebnimi podatki lahko zlonamerneži poskušajo ukrasti celo otrokov denar ali denar njegovih staršev.

Mladoletniki morajo biti zaradi tega še **posebej previdni**, ko prejmejo tovrstno elektronsko pošto in ne smejo **nikoli deliti zaupnih informacij**, tudi če je sporočilo skrb vzbujajoče ali deluje nujno.

NASVETI

Nasveti za učence glede zavarovanja svojih osebnih podatkov:

- Zaklenite svoje naprave tako, da boste edini, ki jih lahko odklene, npr. Z geslom.
- S pregledom zgodovine brskanja v spletnem brskalniku lahko ljudje vidijo, katere spletne strani ste si ogledali. Kadar ne želite, da bi se to zgodilo, lahko vedno izberete ukaz, s katerim si brskalnik ne zapomni iskanih nizov; lahko pa tudi izbrišete zgodovino strani, ki so že shranjene (običajno v zavihku 'orodja').
- Kadar želite na svoj pametni telefon namestiti aplikacijo, vedno preverite, do katerih informacij želi aplikacija dostopati.
- Kadar v elektronski predal prejmete neželjeno pošto ali 'spam', ne smete odpirati prionk – enostavno ignorirajte pošto. Vsebuje namreč lahko povezavo do škodljivih programov.
- Ustvarite **varna gesla** na način, ki vam bo omogočal, da si jih zapomnite:
 - Za geslo ne uporabljajte svojih osebnih podatkov kot npr. svojega rojstnega dneva.
 - Gesel ne shranjujte v bližini svojega računalnika, telefona ali tablice.
 - Poskušajte uporabljati dolga gesla, ki so sestavljena iz različnih vrst posebnih znakov: v gesla vključite male in velike črke, številke, posebne znake.
 - Izogibajte se geslom, ki vsebujejo znake, ki so drug poleg drugega na tipkovnici.
 - Enostavno si boste zapomnili gesla, ki izhajajo iz stavka, kot na primer: Rad Imam Močna Gesla, Ki Skrbijo Za Mojo Zasebnost: RIMGKSZMZ
Ne pozabite se odjaviti, ko uporabljate javne računalnike ali naprave, ki jih delite z drugimi.
 - Ne pozabite redno spreminjati svojega gesla.

- Kadar prejmete elektronsko pošto, ki zahteva kot odgovor vaše osebne podatke, gre morda za prevaro. Vzemite si čas in jo pozorno preberite, preverite vse podrobnosti in ko imate priložnost, na spletu preverite, ali je že kdo drug prejel podobno sporočilo. To lahko storite tako, da v spletni brskalnik vpišete katerega izmed stavkov, ki so navedena v prejetem sporočilu. Zapomnite si, da **ne smete nikoli posredovati svojih gesel** po elektronski pošti. Podjetja ne bodo nikoli zahtevala, da jim zaupne podatke posredujete na tak način, torej po elektronski pošti. Če ste prejeli takšno elektronsko pošto, gre najverjetneje za poskus **ribarjenja podatkov**.

PRIPOROČENE DEJAVNOSTI

1. **Nastavi svojo zasebnost.** Namen te naloge je pomagati učencem razumeti pomen 'nastavitev zasebnosti' pri spletnih storitvah ali aplikacijah, ki jih uporabljajo. Učenci naj:
 - Izberejo spletno storitev ali mobilno aplikacijo, ki jo pogosto uporabljajo in ki vsebuje 'nastavitve zasebnosti' ali različne možnosti določanja zasebnosti. Učenci naj izbirajo med različnimi storitvami ali aplikacijami, da bodo lahko na koncu primerjali ugotovitve. Nekateri učenci lahko delajo tudi skupaj ali v paru na isti napravi.
 - Nato naj **opišejo**, kako storitev deluje, če uporabnik, ko začne uporabljati storitev, ne spremeni nobene od nastavitev zasebnosti. Z drugimi besedami se sprašujemo po tem, kakšne so '**privzete nastavitve zasebnosti**'? Kaj bi se zgodilo, če se uporabnik samo prijavi? So informacije s profila dostopne vsakomur, ki išče podatke s pomočjo spletnih brskalnikov? Ali tak profil vsebuje tudi podatke, kot so uporabnikovo pravo ime, datum rojstva, slika, na kateri je prepoznaven obraz? Kaj se bo zgodilo s podatki ali slikami, ki jih uporabnik pošlje drugim osebam ali po tem, ko jih objavi na takšnem profilu?
 - V naslednjem koraku naj **ugotovijo**, katere možnosti nastavitev zasebnosti so na voljo uporabnikom. Kaj lahko dejansko spremenijo? Lahko nastavijo svoj profil kot zaseben? Lahko delijo informacije samo z nekaterimi osebami? Lahko resnično nadzirajo, kdo bo dostopal do informacij?
 - Če so v razredu otroci, ki ne uporabljajo nobenih spletnih storitev ali aplikacij z nastavitvami zasebnosti, lahko kot alternativo tej nalogi ugotovijo, kakšne so njihove **navade glede delitve informacij v resničnem življenju**. Katere informacije o njih lahko ljudje pridobijo,

ko jih srečajo na ulici? Katere informacije in slike delijo z drugimi? Ali lahko spremenijo svoje 'nastavitve zasebnosti', če bi si to želeli? Kako? Pomislijo lahko na primer na nošenje sončnih očal, deljenje informacij pod pogojem, da druga oseba obljubi, da jih ne bo naprej delila z nikomer ipd.

- V zaključku naloge naj učenci med seboj **delijo, primerjajo** in **se pogovorijo** o svojih ugotovitvah. Obravnavajo lahko naslednja vprašanja: So se v celoti zavedali 'nastavitev zasebnosti' pri storitvah, ki jih uporabljajo? Ali menijo, da jim storitve resnično dovolijo, da nadzirajo svoje podatke? Je pri storitvi ali aplikaciji enostavno najti nastavitve zasebnosti? So te razumljive in jih je enostavno uporabljati?

2. **Kako oblikujemo svojo zasebnost?** Ta naloga je namenjena mlajšim otrokom, z namenom, da premislijo, kako vsakodnevno oblikujejo svoje želje in potrebe glede zasebnosti, torej katera so različna 'orodja' in strategije, ki jih pri tem lahko uporabimo.

- Učenci naj sami ali v manjših skupinah **navedejo** različne skupine oseb, s katerimi delijo različne vrste informacij. To so lahko na primer 1) mama in oče; 2) bratje in sestre; 3) prijatelji; 4) sošolci; 5) učitelji in ostali odrasli, ki jih dobro poznajo; 6) popolni neznanci. Obstajajo lahko tudi druge kategorije, kot npr. 'res najboljši prijatelj', 'sosed', 'stari starši in drugi člani družine', 'najljubša igrača' ipd. Otroci naj sami ugotovijo, katere so tiste skupine, ki so relevantne za njihovo življenje.
- Učenci naj za vsako skupino ljudi **navedejo** tiste informacije, ki jih delijo samo s to skupino. Na primer: Ali obstajajo stvari, ki bi jih povedal samo svojemu (najboljšemu) prijatelju? S kom od navedenih oseb se družijo, ko imajo oblečeno pižamo? Ali mislijo, da obstajajo informacije, za katere je v redu, če jih pozna tvoja učiteljica, ne pa tudi popolni neznanci?
- Razred naj nato **združi** navedene odgovore ter se pogovori o tem, kako se **lahko prepričamo**, da delimo le tiste podatke, ki jih želimo, in le s tistimi osebami, s katerimi jih želimo deliti. Na primer: na ulico ali v trgovino ne gremo v pižami, prijateljem povemo stvari šele takrat, ko drugih ni okoli nas, včasih šepetamo, včasih prosimo ljudi, da obdržijo skrivnost zase ipd.
- Učitelj naj učencem **pojasni**, da zasebnost pomeni nadzor nad tem, kaj posamezni ljudje vedo o nas. Tudi na spletu se moramo, prav tako kot v resničnem življenju, potruditi, da varujemo svoje podatke in jih imamo pod nadzorom.

ZA NAJMLAJŠE

Najmlajši otroci se morajo naučiti, da tako kot obstajajo določeni ljudje, ki bodo morda ukradli naše stvari, obstajajo tudi ljudje, ki lahko ukradejo naše podatke. Zaradi tega morajo biti previdni pri tem, kako ravnajo s svojimi podatki. Premisliti morajo, kje jih hranijo, in jih nikoli ne smejo posredovati neznancem.

ZA STAREJŠE IN/ALI BOLJ ZRELE

Starejši oz. bolj zreli učenci se morajo naučiti odgovornega ravnanja s svojimi podatki. Imeti morajo močna, varna gesla, ohraniti gesla zase in biti pozorni na morebitne primere ribarjenja za podatki. Prav tako morajo dobro poznati 'nastavitve zasebnosti' tistih storitev in aplikacij, ki jih uporabljajo.

8. DRUŽINA, ZASEBNOST IN VARSTVO OSEBNIH PODATKOV

Vloga staršev pri varovanju zasebnosti in osebnih podatkov otrok je izjemno pomembna. Včasih pa lahko tudi preveč posežejo v zasebnost svojih otrok.

CILJI

S tem poglavjem želimo, da bi učenci:

- spoznali, kako jim lahko starši pomagajo pri zaščiti njihove zasebnosti in osebnih podatkov;
- razmislili o tem, ali lahko starši tudi posežejo v njihovo zasebnost in kaj lahko glede tega storijo;
- odkrito razpravljali o teh temah znotraj družine.

KLJUČNI POUČENI

Starši igrajo **ključno vlogo** pri varstvu zasebnosti in osebnih podatkov svojih otrok. Otroci niso vedno sposobni podati privolitve glede uporabe osebnih podatkov, zato so po navadi starši ali skrbniki tisti, ki lahko **podajo privolitev ali zavrniti** uporabo podatkov otrok.

Tudi kadar morajo za obdelavo osebnih podatkov otrok podati privolitev starši, morajo ti pri tem imeti v mislih tudi želje otroka. Starši bi morali poslušati želje otrok pri odločitvi o privolitvi ali zavrnitvi, hkrati pa se z otroki pogovarjati o pomembnih okoliščinah glede obdelave osebnih podatkov, da bodo ti v prihodnosti znali sami **sprejeti prave odločitve**. Starši morajo pomagati otrokom **varovati njihove pravice** in jih naučiti, kako naj to storijo.

Včasih pa se vendarle zgodi, da starši preveč **posežejo** v otrokovo zasebnost in pravico do varstva osebnih podatkov:

- Dolžnost staršev je, da so seznanjeni z dejavnostmi otroka (tudi na spletu), da jih lahko obvarujejo pred nevarnostmi. Ta **nadzor** staršev nad otroki pa je lahko včasih prekomeren in pregloboko poseže v zasebnost otrok. V določenih primerih otroci niti ne vedo, na kakšen način jim starši sledijo, kar je še posebej problematično.
- Starši včasih tudi **'prekomerno'** delijo podatke svojih otrok z drugimi ljudmi. Nekateri starši na primer objavljajo ogromne količine fotografij in videoposnetkov svojih otrok na družbenih omrežjih, pri tem pa ne pazijo na

to, kdo ima dostop do teh podatkov in se ne zavedajo, da lahko slike in posnetki za vedno ostanejo na spletu, povezani z imenom otroka. Fotografije in videoposnetki se morda zdijo staršem ljubki, vendar bi lahko v kakšnih drugih okoliščinah ali kdaj kasneje, otroka spravile v neroden položaj. V najhujšem primeru bi takšne slike in posnetke lahko nekdo celo zlorabil za nezakonite in moralno zavržne dejavnosti.

Otroci bi se morali imeti možnost s svojimi starši ali skrbniki **pogovoriti**, če pride do katerekoli od zgoraj izpostavljenih dilem. Otroci v svojem življenju in za svoj razvoj nujno potrebujejo vsaj okolje, kjer lahko uživajo v **zasebnosti**; prav zato pa se morajo **zavedati** tudi, kako se njihovi podatki uporabljajo. Ko otroci odraščajo, jim morajo dati starši na voljo vedno več možnosti soodločanja glede uporabe njihovih podatkov in jim ponuditi možnost, da izrazijo svoje mnenje glede že objavljenih fotografij, videoposnetkov in preostalih informacij na spletu.

PRIMERI IZ RESNIČNEGA ŽIVLJENJA

Nekateri uporabniki spletne storitve za izmenjavo fotografij **Instagram** so pričeli s trendom **#BabyRP**. V tej igri so posamezniki igrali vlogo 'otroka', 'mame' in 'očeta'. Pri tem so uporabljali fotografije resničnih dojenčkov in otrok, ki so jih dobili od drugih uporabnikov, ne da bi jih prosili za njihovo privolitve. V določenih primerih so starši odkrili, da neznanci uporabljajo slike njihovih otrok šele takrat, ko so bile te že zelo razširjene znotraj izmišljenih družin, z izmišljenimi imeni in izmišljenimi situacijami.

IDEJE ZA POGOVOR

Učence lahko povabite k pogovoru o različnih temah:

1. **Osebne izkušnje.** So se otroci že kdaj počutili, da so starši posegli v njihovo zasebnost in kdaj? Kaj so glede tega storili? Včasih starši posežejo v otrokovo zasebnost, ne da bi se tega sploh zavedali. Starši lahko na primer med večerjo z družinskimi člani ali prijatelji delijo anekdoto o otrokovem življenju, za katero mislijo, da je ljubka ali zabavna, otroka pa je ob tej zgodbi neizmerno sram. Otroci se lahko ob tem pogovorijo, ali menijo, da imajo starši enako predstavo o tem, kaj morajo ohraniti kot zasebno.
2. **Meje starševskega nadzora.** Ali menite, da imajo starši pravico nadzirati vaše aktivnosti? Zakaj naj bi to počeli? Ali mora imeti tak nadzor svoje meje? Ali se morajo pravila razlikovati glede na starost ali zrelost otroka?

PRIPOROČENE DEJAVNOSTI

1. **Sprejemljive prakse.** Ta vaja bo spodbudila učence k premisleku o tem, kaj njihovi starši vedo o njih in njihovem vedenju. Učenci naj:
 - **naštejejo** načine, na katere lahko starši sledijo njihovim aktivnostim. Razmislijo lahko na primer o pregledovanju spletnega obnašanja, nadzoru uporabe pametnih telefonov, dostopu do njihovih profilov na družbenih omrežjih, pregledu nad porabo njihovega (elektronskega) denarja ipd.
 - **Premislijo in izrazijo**, katere od teh dejavnosti za njih niso sprejemljive.
 - **Primerjajo** svoje odgovore z odgovori sošolcev. V primeru, da prihaja do večjih razlik, naj se o njih pogovorijo.
2. **Uporaba otrokovega znanja.** Za starše je lahko učenje otrok o zasebnosti na spletu in zaščiti osebnih podatkov zelo zahtevno, saj nimajo dovolj znanja o elektronskih napravah in storitvah, ki jih otroci dnevno uporabljajo. S to nalogo lahko učence spodbudimo, da o tej težavi razmislijo in ugotovijo, da imajo tudi oni pomembno znanje, ki ga lahko delijo s svojo družino. Učenci lahko sami ali v manjših skupinah poskusijo naslednjo nalogo:
 - Učenci naj **zasnujejo učno uro za starše** o določeni napravi, platformi družabnega omrežja, aplikaciji ali katerikoli drugi spletni storitvi, ki jo dobro poznajo in jo radi uporabljajo, njihovi starši pa te naprave oz. storitve ne uporabljajo oz. jo slabo poznajo. Kaj bi morali starši vedeti, če bi jo uporabljali? Za kaj je uporabna? Zakaj jo radi uporabljamo? Opišejo naj njene funkcije in njene prednosti.
 - **V učno uro naj vključijo nasvete o zasebnosti** za starše, da bodo ti lahko poskrbeli za svojo zasebnost in svoje osebne podatke pri uporabi te storitve. Je bolje, da se v storitev prijavijo s svojim pravim imenom ali z vzdevkom? Obstajajo nastavitve zasebnosti, ki jih lahko prilagodijo? Ali bo podjetje o njih zbiralo kakšne podatke? Kdo bo videl informacije, ki jih bodo delili?

ZA NAJMLAJŠE

Najmlajši otroci morajo razumeti, da imajo starši ključno vlogo pri zaščiti njihovih osebnih podatkov in zasebnosti na spletu. Kadar imajo občutek, da starši posegajo v njihovo zasebnost ali ne varujejo njihovih pravic na način, kot bi si sami želeli, se morajo o tem z njimi pogovoriti. Starši imajo morda dober

razlog za to, kar so storili, morda pa se v določenih primerih le niso zavedali, da s tem posegajo v zasebni prostor otroka.

ZA STAREJŠE IN/ALI BOLJ ZRELE

Starejši učenci morajo razumeti, da imajo starši ključno vlogo pri zaščiti njihove zasebnosti in osebnih podatkov, vendar naj se zavedajo tudi, da imajo pri tem pomembno vlogo tudi sami. Tudi njihov pogled na zasebnost in varstvo osebnih podatkov šteje.

9. BODI VAREN IN SE DOBRO IMEJ

Pri uporabi interneta lahko naletimo na škodljive vsebine in se srečamo z ljudmi, ki niso prijazni ali uvidevni; nekateri imajo celo slabe namene. Otroci se morajo v največji možni meri izogniti nevarnostim, ki jih je mogoče predvideti, in se izogibati ravnanju, ki lahko škodi drugim.

CILJI

To poglavje bo učencem pomagalo:

- spoznati možne nevarnosti spleta;
- razmisliti o 'spletnem nadlegovanju' in o 'sovražnem govoru' na spletu;
- razmisliti o možnih nevarnostih deljenja eksplicitnih vsebin, t. i. 'seksting';
- preprečiti tvegano vedenje.

KLJUČNI POUČENI

Kot v resničnem življenju tudi na spletu niso vsi ljudje naši prijatelji. Na družabnih omrežjih, pri igranju spletnih iger ali pri komentiranju spletnih vsebin lahko naletimo na osebe, ki sicer delujejo prijazno, a to še ne pomeni, da jim lahko zaupamo. Otroci in najstniki se morajo zavedati, da z neznanci na spletu ne smejo deliti svojih zaupnih informacij, kot tega ne počnejo z neznanci na ulici. Še posebej ne smejo deliti svoje **telefonske številke** ali **naslova**, ki bi ga lahko osebe kasneje uporabile za nadlegovanje.

Prijatelji na spletu nas lahko prizadenejo tako kot prijatelji v resničnem življenju. Na spletu se včasih obnašamo celo drugače, kot bi se v živo, morda zato, ker nas nihče ne vidi, ali pa se ne zavedamo vseh posledic svojega obnašanja na spletu.

Včasih žal namenoma prizadenemo drug drugega. '**Spletno trpinčenje in nadlegovanje**' je neželena ali celo kazniva uporaba spleta z namenom nadlegovanja, ustrahovanja ali drugega škodljivega ravnanja, navadno pa oseba trpinči in nadleguje druge namenoma in večkrat. Obstaja več vrst spletnega trpinčenja in nadlegovanja, od širjenja lažnivih govoric po družbenih omrežjih do nenehnega nadlegovanja, trpinčenja in ustrahovanja.

To obnašanje ima lahko **hude posledice** za žrtev. Zato je zelo pomembno, da otroci ne sodelujejo v nobeni dejavnosti (od objavljanja, komentiranja do deljenja vsebin), ki bi jih nekdo lahko razumel kot spletno trpinčenje ali

nadlegovanje. Prav tako je pomembno, da otroci stojijo ob strani vrstnikom, ki so doživeli spletno trpinčenje oz. nadlegovanje. Kadar otrok doživlja spletno trpinčenje in nadlegovanje, pa mora imeti na voljo starša, skrbnika ali drugo odgovorno odraslo osebo, ki bo lahko takšno ravnanje takoj **ustavila** oz. preprečila.

Posebej sramoten način spletnega nadlegovanja so napadi na osebo zaradi določene njene osebne okoliščine, denimo zaradi spola, etične ali verske pripadnosti, telesne pomanjkljivosti, spolne usmerjenosti ali katerekoli lastnosti, zaradi katere zmotno menijo, da upravičuje njihovo nadlegovanje. To včasih poimenujemo '**sovražni govor**', ki ni škodljiv le za napadeno osebo, temveč za celo skupino (običajno ranljivih) oseb, na katero se nanaša. Otroci se morajo zavedati, da je sovražni govor kazniv in da ga morajo prijaviti vedno, ko se z njim srečajo.

Učenci naj razmislijo o možnih nevarnostih sekstinga - izmenjave eksplicitnih vsebin spolne narave (fotografije, sporočila, videoposnetki), tako po kratkih sporočilih, elektronski pošti ali družbenih omrežjih. Najstniki, ki se znajdejo v skušnjavi, da bi si izmenjali takšna sporočila, običajno nimajo predstave o vseh možnih načinih, kako bi ta sporočila lahko končala v rokah napačne osebe. Opozoriti jih je torej treba, da lahko kdorkoli, ki na kakršenkoli način pride v stik s takšno vsebino, to deli naprej ali jo celo javno objavi. Pri tem ni nujno, da to stori z **namenoma**, lahko je le **malomaren, deli vsebino po pomoti ali kot (slabo) šalo**. Najstniki si običajno ne morejo predstavljati vseh možnih **negativnih posledic** takšnih situacij, zaradi katerih se lahko znajdejo v zelo ranljivem položaju in so izpostavljeni sramotenju ali izsiljevanju.

IDEJE ZA POGOVOR

1. **Osebne izkušnje spletnega trpinčenja in nadlegovanja (in kako ga ustaviti).** Učenci naj se pogovorijo o naslednjih vprašanjih: So se že kdaj srečali z ravnanjem, ki so ga prepoznali kot 'spletno trpinčenje in nadlegovanje'? Kaj so storili? Strokovnjaki pravijo, da je treba v takšnih trenutkih žrtvi pokazati, da ji stojimo ob strani in da nas takšno spletno trpinčenje in nadlegovanje ne ustrahuje. Je to lahko storiti? Kaj lahko v takšnih situacijah še naredimo?
2. **Najbolj intimne vsebine.** Učenci naj se pogovarjajo o nevarnostih, povezanih s sekstingom, pri čemer naj razmislijo o naslednjih scenarijih:
 - **Situacija:** Dekle "D" in njen fant "F", oba sta bila najstnika, sta se odločila praznovati svojo obletnico tako, da si bosta izmenjala svoje gole

fotografije, saj sta prebrala, da je to lahko zabavno. Obljubila sta si, da fotografij ne bosta pokazala nikomur. Naslednji dan fant F na kopališču v trenutku nepazljivosti pusti svoj telefon na vrhu garderobne omarice. Njegov znanec opazi telefon, preveri vsebino in se odloči, da bo sliko dekleta objavil na priljubljenem družbenem omrežju, v katerega se prijavi z računom fanta F. Znanec telefon nato vrne tja, kjer ga je našel. Dekle D se doma spravi k pisanju bloga, na katerem bi pisala o tem, kako se je imela na počitnicah. Nenadoma pa zagleda svojo golo fotografijo, ki jo je domnevno objavil njen fant F. Skoraj takoj se pod sliko pojavljajo zasmehujoči in ponižujoči komentarji od različnih oseb, tudi od tistih, ki niso spletni 'prijatelji' njenega fanta F. Dekle D je zaradi situacije tako jezna in prizadeta, da se odloči, da se bo maščevala na način, da bo na svojem blogu, do katerega lahko dostopa kdorkoli, objavila fotografijo fanta F, hkrati pa jo pošlje tudi njegovemu očetu (katerega naslov e-pošte najde na spletu).

- **Pogovor:** Kaj bi se lahko z bivšima zaljubljenecema zgodilo v nadaljevanju? Kaj bi lahko D in F storila, da bi se tej situaciji izognila? Ali menite, da bi se takšna situacija lahko zgodila tudi v resničnem življenju? Če ne, katere podobne situacije si lahko zamislite?

PRIPOROČENE DEJAVNOSTI

1. **Pomisl preden deliš.** Otroci in najstniki objavljajo neprimerne vsebine iz mnogo različnih razlogov, pogosto pa tako, da sploh ne razmislijo o možnih posledicah. Otroci lahko mislijo, da je zabavno, če delijo sliko prijatelja, ki izgleda smešno ali čudno, ne da bi se zavedali nevarnosti, da bodo drugi uporabniki spleta to informacijo znova in znova delili naprej. Velikokrat se ne zavedajo tega, da tako široka izpostavljenost prijateljem morda ne bo smešna. Otroci lahko morda v trenutku jeze na spletu objavijo posebej zlobne informacije o nekom, ne da bi se pri tem zavedali, da s tem ne bodo zgolj prizadeli te osebe, temveč bodo lahko resno škodovali njenemu življenju in duševnemu miru. Naslednja naloga učence spodbuja k **razmisleku** o takih situacijah. Učenci naj:

- **Opišejo** situacijo, v kateri nekdo na spletu objavi ali deli informacijo, ki bi lahko pozneje osebi povzročila probleme. Učenci naj povejo, katere so tiste informacije, ki bi lahko bile problematične. Na primer: najstnik deli fotografije z zabave, ki naj bi bile poznane le tistim, ki so bili na zabavi; prijatelj, s katerim se spreš, deli z drugimi tvoje skrivnosti.

- **Pogovorite se**, kaj bi lahko storili za to, da bi te probleme preprečili? Ali obstajajo kakšne vrste podatkov, ki jih oseba ne sme nikoli in z nikomer deliti? Ali menijo, da je dobra ideja, da pred objavo podatkov o drugi osebi to vedno prosiš za soglasje?

ZA NAJMLAJŠE

Najmlajši otroci morajo razumeti, da lahko na spletu srečajo vse vrste ljudi. Tudi kadar ti neznanci ali novi 'prijatelji' delujejo prijazno, ne moremo vedeti, ali jim lahko popolnoma zaupamo. Otroci ne smejo neznancem ali spletnim 'prijateljem' nikoli zaupati svoje telefonske številke, naslova ali kakšne svoje slike.

ZA STAREJŠE IN/ALI BOLJ ZRELE

Starejši ali bolj zreli otroci morajo osvojiti bolj kritičen odnos do svojega spletnega obnašanja. Vedno se morajo vprašati, ali bi lahko imela informacija, ki jo želijo objaviti ali deliti, za njih ali koga drugega negativne posledice, na primer, če bi jo uporabili za drugačen namen od prvotnega.

10. KAKO UKREPATI?

Pravica do varstva osebnih podatkov pomeni, da imajo posamezniki pravice, ki jih lahko uporabijo – sami ali s pomočjo odrasle osebe. Če se pri izvrševanju pravic pojavi kakšen dvom ali težava, se posameznik vedno lahko obrne na organ za varstvo osebnih podatkov; v Sloveniji je to Informacijski pooblaščenec. Dobro je, da vsakdo ve, na koga se lahko obrne tudi v nujnih primerih.

CILJI

S tem poglavjem bodo učenci:

- osvojili znanje o **pravica**h glede varstva osebnih podatkov;
- spoznali, kaj narediti, kadar neka organizacija ne spoštuje njihovih pravic;
- spoznali delo **organa za varstvo osebnih podatkov**;
- ugotovili, **na koga se lahko obrnejo** v nujnih primerih.

KLJUČNI POUČENKI

Vsak posameznik ima pravico od podjetja ali organizacije, ki obdeluje njegove osebne podatke, zahtevati informacijo o tem, **katere** njegove **osebne podatke** obdeluje, zahtevati **popravek**, če so podatki nepopolni ali napačni, ali zahtevati **izbris** podatkov, če ni potrebe po tem, da jih podjetje obdeluje.

Kadar oseba **privoli**, da podjetje obdeluje njene osebne podatke, pa si kasneje premisli, ima pravico zahtevati od podjetja, naj takoj preneha obdelovati njene podatke. To so **temeljne pravice varstva osebnih podatkov**, ki jih lahko kdorkoli uveljavlja v razmerju do podjetij ali organizacij, ki obdelujejo njegove osebne podatke.

Kadar določeno podjetje ponuja storitve ali izdelke po telefonu ali elektronski pošti, lahko zahtevamo, da tega **ne počne več**. Velikokrat je to mogoče z 'odjavo' od prejemanja elektronske pošte. Vsa oglasna sporočila morajo vsebovati podatek o pošiljatelju in jasna navodila o tem, kako se od njih odjaviti.

Najmlajši otroci ne morejo sami uveljavljati svojih pravic glede varstva osebnih podatkov, zato morajo za njihovo uporabo prositi **starše, skrbnike ali drugo odgovorno odraslo osebo**.

Kadar podjetje ali organizacija ne odreagira na našo zahtevo in ne spoštuje naše odločitve glede osebnih podatkov, se lahko obrnemo na **organe za varstvo osebnih podatkov**.¹ Organ za varstvo osebnih podatkov skrbi za to, da vsi obdelujejo osebne podatke v skladu z zakonom in da podjetja ali organizacije spoštujejo odločitve posameznikov glede njihovih osebnih podatkov.

Organi za varstvo osebnih podatkov lahko svetujejo in če je treba, lahko pomagajo tudi pri vložitvi pritožbe. V določenih primerih lahko tudi stopijo v stik s podjetjem ali organizacijo in pomagajo rešiti nastalo težavo.

Določene situacije narekujejo **nujno ukrepanje**, a organi za varstvo osebnih podatkov v takšnih situacijah morda ne morejo posredovati. Otroci lahko odkrijejo, da je nekdo delil njihove osebne podatke, ki so zelo občutljivi in jih je treba takoj odstraniti. Včasih se to zgodi po pomoti, včasih pa zaradi slabih namenov osebe, ki ne želi sodelovati pri izbrisu podatkov.

V takih primerih lahko otroci ali najstniki zahtevajo izbris podatkov tako, da kontaktirajo spletno stran ali ponudnika določene spletne storitve. Ker je to včasih zahtevno, jih ne sme biti strah prositi za pomoč **starše, skrbnike ali druge odgovorne odrasle osebe**, ki jim lahko pomagajo.

Otroci lahko v teh primerih pokličejo tudi na **telefonske številke za otroke in mladostnike v stiski**. To so klicne številke, ki so specializirane za pomoč otrokom in najstnikom, ki se znajdejo v zahtevnih situacijah na spletu ali se srečajo z neprimerno vsebino. Običajno so te storitve brezplačne in anonimne.² Pomoč lahko nudijo tudi v primeru **spletnega nadlegovanja**. V zelo resnih primerih pa naj se otroci obrnejo na **policijo**.

V Sloveniji se otroci lahko obrnejo za pomoč na Safe-si (www.safe.si), Spletno oko (www.spletnooko.si) in na Telefon za otroke in mladostnike - TOM (116111).

¹ Vsi organi za varstvo osebnih podatkov po posameznih državah, so navedeni na naslednji povezavi: http://ec.europa.eu/justice/data-protection/bodies/authorities/eu/index_en.htm. Spletna stran Informacijskega pooblaščenca je <https://www.ip-rs.si/>.

² Vse nacionalne številke za pomoč otrokom v stiski so navedene na naslednji povezavi: <http://www.saferinternet.org/helplines>.

PRIPOROČENE DEJAVNOSTI

1. **Uporaba pravic v resničnem življenju:** Ta naloga lahko zahteva nekaj časa (vsaj nekaj tednov za prejem vseh odgovorov), vendar je lahko zelo uporabna za to, da učenci dejansko doživijo, kaj pomeni imeti pravico do varstva osebnih podatkov. Vsak učenec naj:
 - **Izbere** podjetje ali organizacijo, za katero meni, da ima njegove osebne podatke.
 - **Napiše**, zakaj je izbral to podjetje ali organizacijo in katere njegove podatke meni, da obdeluje.
 - **Uporabi svojo pravico do seznanitve**, tako da kontaktira podjetje ali organizacijo in jo zaprosi za podatek o tem, katere njegove podatke zbira.
 - **Počaka na odgovor** nekaj tednov (v Sloveniji je rok za odgovor na takšno zahtevo 15 do 30 dni, odvisno od tega, kaj posameznik zahteva).
 - V razredu **pojasni**, katero organizacijo je kontaktiral, zakaj, katere njegove podatke naj bi imela, ali je prejel odgovor in kaj ga je v odgovoru presenetilo.
 - **Primerja** svojo izkušnjo z izkušnjami sošolcev. Ob upoštevanju vseh izkušenj lahko učenci poskušajo premisliti o naslednjih vprašanjih: Ali je bila vaja uporabna? Zakaj? Ali je bilo enostavno prejeti odgovor? Ali bi lahko zaprosili za dodatno pomoč organ za varstvo osebnih podatkov?

ZA NAJMLAJŠE

Najmlajši otroci morajo vedeti, da jim lahko pri **izvrševanju njihovih pravic pomagajo** starši ali odgovorna odrasla oseba. Poznajo naj obstoj **organa za varstvo osebnih podatkov**, ki skrbi za to, da vsi spoštujejo pravila glede varstva osebnih podatkov. Zavedajo naj se, da je bolje prositi za pomoč, kadar se na spletu srečajo z neprimerno vsebino.

ZA STAREJŠE IN/ALI BOLJ ZRELE

Starejši učenci morajo poznati svoje **pravice glede varstva osebnih podatkov** in ne sme jih biti strah le-te tudi **uporabiti**. Razumeti morajo, da morajo ukrepati, ko nekdo zlorablja njihove osebne podatke in da obstaja **organ za varstvo osebnih podatkov**, ki jim lahko nudi dodatne informacije in pomoč. Naučiti se morajo prositi za pomoč odraslo osebo, kadar so v težavah zaradi določene spletne vsebine.

MINI LISTINA PRAVICE DO ZASEBNOSTI IN VARSTVA OSEBNIH PODATKOV

Mini listina vsebuje temeljne pravice, ki jih po evropski zakonodaji uživajo vsi otroci in mladostniki.



Imaš pravico do zasebnosti. Vsi imamo pravico do zasebnosti od rojstva dalje. »Vsi« pomeni tudi dojenčki, otroci in mladostniki. Odrasli imajo prav tako pravico do zasebnosti.

Imaš pravico do varstva svojih osebnih podatkov. Nihče ne sme obdelovati podatkov drugih ljudi brez upoštevanja določenih pravil kot na primer, da je treba obdelovati čim manj osebnih podatkov, in da jih je treba hraniti na varnem. S tem, ko podjetja in druge organizacije obdelujejo osebne podatke, lahko zase pridobivajo pomembne koristi in s tem tudi čedalje več moči. Pravila varstva osebnih podatkov nam pomagajo, da smo mi in naši osebni podatki varni in pod nadzorom.

Vsi tvoji osebni podatki si zaslužijo varstvo. Ni važno, če so podatki že javni, morda zato, ker si nekega dne soglašal s tem, da jih deliš z drugimi. Ni važno, če

podatki niso nikoli bili »najvišja (državna) tajnost« ali pa, če se ne zdijo posebej intimni ali občutljivi. Kadarkoli nekdo obdeluje podatke o tebi, mora spoštovati pravila. Celo dolgotrajni in običajni podatki lahko ljudem povzročijo težave.

Imaš pravico vedeti, kdo ima podatke o tebi, zakaj jih uporablja in kako jih uporablja. Upravičen si do tega, da imaš vsaj nekaj nadzora nad tem, kaj se dogaja s tvojimi osebnimi podatki, to pa je možno le, če si obveščen o tem, kdo uporablja podatke, zakaj in kako. Torej imajo tisti, ki želijo obdelovati tvoje podatke obveznost, da te o vsem tem tudi obvestijo.

Imaš pravico, da pridobiš jasne in popolne informacije. Vedno moraš biti sposoben razumeti, kaj ti je upravljavec podatkov povedal o obdelavi tvojih podatkov. Pojasnila morajo biti pregledna, zaradi česar jim ne dovoli, da kaj prikrivajo. Če kaj ni jasno, si drzni vprašati za pojasnila!

Imaš pravico, da veš natančno, katere podatke o tebi imajo. Predstavljaljaj si, da ti povedo, zakaj želijo tvoje podatke in kako jih bodo uporabili. Ali, da so te o tem morda pozabili obvestiti. Ali pa, da gre za zares nepomembne podatke. V vsakem primeru jih lahko vprašaš, kaj vedo o tebi, in dolžni so ti povedati.

Imaš pravico do popravka netočnih podatkov o sebi. Včasih je lahko velik problem, če imajo ljudje napačne informacije o tebi. To jih vodi v napačne zaključke in zaradi tega lahko sprejemajo tudi napačne odločitve, ki se tičejo tebe. Če opaziš, da imajo napačne podatke, lahko zahtevaš njihov popravek, kar so dolžni storiti.

Imaš pravico, da si slišan. Včasih so podjetja in druge organizacije dolžne obdelovati določene podatke o tebi. Toda pogosto nimajo nobenega utemeljenega razloga oziroma podlage za to in zato te bodo vprašala za tvoje soglasje. Odrasli in starejši mladoletniki imajo pravico do privolitve v določeno obdelavo osebnih podatkov. Če si mlajši mladoletnik, verjetno ne boš privolil sam, ampak bodo odločitev o privolitvi sprejeli tvoji starši. Toda pred tem bi se morali starši posvetovati tudi s tabo in ugotoviti, kaj o tem misliš ti.

Imaš pravico, da se pritožiš. Če nekdo ne spoštuje pravil, ga seznanjaj s tem, da poznaš svoje pravice. Če temu ne bodo sledili, zaprosi nekoga za pomoč in pri tem vztrajaj! Organi za varstvo osebnih podatkov so bili ustanovljeni v vsaki državi zato, da bi pomagali ljudem pri težavah v zvezi z njihovimi osebnimi podatki.

Sedaj, ko poznaš svoje osnovne pravice, poskrbi

... da jih boš uporabljal! Gospodar svoje zasebnosti in pravic varstva osebnih podatkov boš postal le, če boš te pravice izvrševal. Ljudje zbirajo podatke o nas vsak dan, zato naj ti postane navada, da razmišljaš o tem, kdo kaj zbira in kako to počne, kako podatke uporablja in za kakšen namen.

... da jih boš uporabljal pametno! Pravice so nam podeljene v uporabo zato, da so naši podatki varni in ne zato, da z njimi popravljamo nepremišljeno vedenje. Najboljši način, da ne izgubiš nadzora nad svojimi podatki je, da dobro premisliš, preden jih deliš z drugimi.

... da si boš zapomnil, da imajo drugi ljudje točno enake pravice kot ti. Zato poskrbi, da jih boš spoštoval, na primer tako, da ne razširjaš fotografij, na katerih so drugi ljudje ali informacij o njih, ne da bi jih prej vprašal, ali se s tem strinjajo. Bodi prijazen in vljuden, tudi na internetu.

PREDSTAVITEV IZBRANIH UČNIH UR

Priročnik za učitelje je bil zamišljen tudi kot vabilo za učitelje, da pripravijo svoje načrte učnih ur, ki bi bili pisani na kožo njihovim študentom. V projektu ARCADES so nadzorni organi za varstvo osebnih podatkov iz Poljske, Slovenije in Madžarke pripravili natečaje za učitelje, ki so lahko prijavi svoje načrte učnih ur, da bi jih delili širše in bi jih lahko uporabljali tudi njihovi kolegi v drugih državah. Vsak nadzorni organ je izbral zmagovalca v nacionalnem natečaju, zmagovalne ure pa so predstavljene v tem priročniku, skupaj z uvodnimi besedami njihovih avtorjev.

Nagrajene učne ure odlikavajo različne pristope k poučevanju o zasebnosti in varstvu osebnih podatkov: Prvi načrt učne ure, *Mali škratje*, ponuja scenarij za mlajše otroke in osnovna načela pri deljenju podatkov na spletu podaja na igriv način. Drugi načrt učne ure, *Kdo želi tvoje osebne podatke?*, je namenjen starejšemu občinstvu in stremi k prikazu širše slike obdelave osebnih podatkov. Zadnji, tretji učni načrt, *Spletne nevarnosti*, pa je osredotočen za zavedanje o spletnih tveganjih.

1. PRIMER UČNE URE 1: MALI ŠKRATJE

Nina JELEN

1.1. NAJBOLJŠE ŠOLSKO LETO

To leto je bilo za našo šolo iz Podkuma, OŠ Ivana Skvarče Zagorje, resnično uspešno. Izpeljali smo kup projektov, bili pri tem uspešni, hkrati pa smo se zabavali in ogromno naučili. In ko smo se ravno pripravljali na bolj umirjeno obdobje, ko se naj bi posvetili samo golemu pouku in se malo umirili, se nam je pripetila nagrada za najboljšo učno uro Informacijskega pooblaščenca. In naše leto še bolj postavila na glavo. Šolo so preplavili škratki iz pesmice, škratje pesmice in plesi, ki so bili del učne ure... skratka eno samo veselje.

In ne samo to; naša majhna, vaška podružnična šola je kar naenkrat postala slavna v Sloveniji. Oklicali so nas za »najboljšo šolo«, »najbolj uspešno«, o nas so pisali prekrasne članke, snemali televizijske in radijske oddaje. Postali smo velike male zvezde. Tako kot naši škratki v zgodbi... na dober način, seveda.

V resnici si niti v sanjah nisem predstavljala, da bomo zmagali. Glede na to, da so pri projektu sodelovale tudi srednje šole in starejši učenci, se mi je zdelo, da bomo premajhni. Še ko sem prosila ravnateljico, da mi podpiše vse listine za natečaj, sem jo pospremila s stavkom: »Saj ne bo nič iz tega, pa bom vseeno poslala, ker se mi ura sicer zdi koristna. Mogoče jo bodo pa vseeno lahko kje uporabili.« Zato je bilo veselje še toliko večje, ko sem prejela klic Informacijske pooblaščenke, ki je naznanila, da smo v Sloveniji zmagali. Mi – ta najmanjši!

Prepričana sem, da je treba o življenju na spletu spregovoriti že z malimi otroki. Otroci so še naivni, ne zavedajo se, kako je splet širok, kako tam – tako kot v resničnem življenju – lahko naletiš na dobre in slabe ljudi. Preden sem izvedla učno uro, so bili moji učenci pripravljani na spletu deliti vse svoje podatke – svoj naslov, telefonsko številko, nekateri bi zapisali še številko bančne kartice, če bi jo le imeli. Uporabo spleta je nemogoče prepovedati in tudi ni prav, da se prepove, saj nam splet prinaša številne koristi, ugodnosti, znanje. Je pa treba otroke na ta del življenja pripravljati, tako kot jih pripravljamo na resnično življenje.

Vesela sem, da sem se lotila tega projekta, tudi če ne bi dobili nagrade. Menim, da so se otroci pri učni uri veliko naučili. Če bodo o varni uporabi spleta poslušali še v naslednjem šolskem letu ter v vseh letih kasneje, verjamem, da se bodo na naša

spletna pravila spomnili tudi takrat, ko bodo postali pravi in aktivni uporabniki spleta.

Zelo sem hvaležna za vse, kar se nam je zgodilo. Mislim, da se ti takšna nagrada in vse to dogajanje okoli nje zgodi samo enkrat v življenju. Še posebej sem hvaležna Informacijskemu pooblaščenču za vse, kar so pripravili za nas. Učenci in jaz smo izkusili doživetja, ki se najbrž marsikomu izmed nas ne bodo zgodila nikoli več. Igrali smo na pravem ljubljanskem odru, dobili knjižice, tablične računalnike. Videli in predstavili smo se v televizijskem studiu, izkusili, kako se snema radijska oddaja in kako se napiše pravi časopisni članek. Odpotovali smo v Barcelono, kar je bilo resnično neverjetno doživetje!

Naša mala šola je postala velika. Dokazali smo, da čeprav smo majhni in nas ni veliko, imamo čisto vse, kar imajo veliki. Še enkrat... najlepša hvala!

1.2. NAČRT UČNE URE

1.2.1. Opis

Tema	Varstvo zasebnosti in osebnih podatkov na internetu
Trajanje	45 minut
Razred	2. razred
Starost	7 in 8 let
Cilji	Razumeti pomen varstva osebnih podatkov. Naučiti se prepoznati »osebne podatke« in razumeti, zakaj jih je treba varovati. Spoznati pojem »občutljivih osebnih podatkov«, oziroma podatkov, ki potrebujejo posebno zaščito. Povečati ozaveščenost o pravicah, ki v zvezi z osebnimi podatki pripadajo vsakemu posamezniku. Spoznati možne nevarnosti spleta.
Oblike poučevanja	Individualno, skupinsko, frontalno.

Metode dela	Pogovor, razlaga, demonstracija, dramatizacija, metoda branja in dela s tekstom.
Učni pripomočki	Pesem (avtorica Nina Jelen) Pripomočki za dramatizacijo: kape za škrate, fotoaparati, predpasnik, izvijač, plesna obleka... Učni list: obrazec za registracijo na lažni spletni strani faceinfaconi.com

1.2.2. Potek učne ure

Uvodna motivacija	
Učitelj	Učenci
<p>Učitelj učencem doživeto prebere zgodbo »Škratice in možički za grički« (glej spodaj) in zraven pokaže ilustracije.</p> <p>Zgodbo obnovijo.</p> <p>Kdo so bili škratke in možički?</p> <p>Kakšni so bili?</p> <p>So bili dobri ali slabi?</p> <p>Zakaj so jih druga bitja rada obiskovala? (preberejo del, ki opisuje, zakaj so bitja tako rada prihajala k njim).</p> <p>So imeli tudi kakšne smešne navade? Kakšne?</p> <p>Kaj je storil Fotko? Je naredil prav, da je objavil posnetek?</p> <p>Kako so se takrat počutili škratinje in možički?</p>	<p>Učenci poslušajo in se vživijo v zgodbo.</p> <p>Učenci aktivno sodelujejo v pogovoru in obnavljajo zgodbo.</p>

<p>Zakaj so jih druga bitja takrat rada obiskovala? (preberejo del, ki opisuje, zakaj so bitja po neljubem dogodku tako rada prihajala k njim).</p> <p>Učitelj poudari, da kar nekdo naloži na splet, ZA VEDNO ostane na spletu.</p> <p>Kako se je zgodba končala?</p>	
<p>Glavni del ure</p>	
<p>Učitelj učencem projicira sliko novega družbenega omrežja Faconi in Faconke, izmišljene spletne strani za mlajše otroke, kot so oni. Ponuja vrsto iger, klepet z drugimi otroki in druge zabavne aktivnosti.</p> <p>Ne da bi jih prej opozoril, učitelj razdeli učne liste, z obrazcem za prijavo na novo spletno stran Faconiinfaconke.com. Prijavnica od njih zahteva veliko osebnih podatkov.</p> <p>Navodilo učencem: Izpolni tiste podatke, za katere meniš, da so primerni za na splet in bi jih brez skrbi objavil na spletu. Ko izpolnijo prijavnico, se z učiteljem pogovorijo o podatkih, ki so jih bili pripravljene deliti na spletu. Počasi obdelajo vsak podatek, ki so ga vnesli v prijavnico.</p> <p>Učitelj poudari, da učenci na spletu ne smejo izdajati osebnih podatkov (ime, priimek, naslov, rojstni datum, telefonska številka, e-naslov, geslo, podatki o starših, podatki o krajih, kjer se zadržujejo). Prav tako naj ne objavljajo svojih ali posnetkov prijateljev.</p>	<p>Učenci izražajo mnenja o spletni strani. Jih mika, da bi se prijavi ali ne?</p> <p>Učenci samostojno izpolnjujejo učne liste – prijavnico za spletno stran Faconi in Faconke.</p> <p>Učenci sledijo pogovoru in na svoji prijavnici zapišejo klicaj, kjer so izpolnili podatke, pa bi bilo bolje, da jih ne bi.</p>

Učitelj pove, da imajo vsi do svojih podatkov posebne pravice in da je osebne podatke treba varovati. Pove, da to lahko izkoriščajo razna podjetja in trgovine.

Učitelj posebej poudari pomen varnosti.

Tako kot v realnem življenju so tudi ljudje na spletu lahko hudobni. Zato naj nikoli ne zaupajo tistim, ki jih ne poznajo. Na spletu se lahko nekdo izdaja za nekoga drugega. Saj so videli, kako so se druga bitja v zgodbici norčevala iz škratic in možičkov.

Učitelj razloži, da morajo učenci poleg za svojo varnost skrbeti tudi za svojo identiteto na spletu.

Tako kot se v resničnem življenju trudijo, da so dobri, pridni, urejeni, morajo skrbeti za svojo podobo tudi na spletu. So druga bitja po objavi posnetka videla, da so škratki v resnici zelo dobri, prijazni in pridni?

Skrbeti pa morajo tudi za podatke prijateljev in znancev. Zato je Fotko naredil zelo narobe, ko je objavil posnetek svojih someščanov, ne da bi jih prej vprašal.

Učitelj predstavi še razredni plakat: Zlata pravila Fac in Faconov in internetu. Plakat obesijo v razredu.

Učenci delijo svoje izkušnje.

Zaključni del ure

Učenci dramatizirajo zgodbico Škratice in možički za grički. V igro se vživijo in jo čim bolj doživeto zaigrajo.

1.2.3. Učni pripomočki

1.2.3.1. Pesem

Škratice in možički za grički (oziroma, kako so se mali škratje osramotili)

Za daljnimi grički,
v majhni vasički,
so živele ljubke škratice in skuštrani možički.

Bili so si malo podobni in malo različni,
veseli, iskreni, preprosti,
nikdar zlobni,
nikdar sebični.

Od blizu in od daleč preplezali so gričke, da bi videli te ljubeče škratice in možičke.

Vsi so jih občudovali, vsi so se z njimi smejali.

Najbolj priden je bil škratek Pepe,
vedno je delal, vedno po mašinah brkljal,
zraven pa se prav zadovoljno smehljajal.
Res pa je, da je imel Pepe
vedno polna ušesa mastne repe.
Kar naprej je brskal in vrtal po njih,
da je v njegovi glavi včasih nastal pravi prepih.
Dobrodušen Smrdec je rad priskočil na pomoč,
sosedu je pokosil travo, če je bil dan ali pa noč.
Smrdec pa je sem in tja spustil smrdljiv in glaaaaaasen prdec.
»Najprej zdravje, potem kultura« je trdil,
ko kakšen škrat ob njem, se je od smrada in slabosti zvil.

Kuštroglavec Spak je zabaval mlade in stare,
ker je pokal take smešne šale.
In vice,
da so se od smeha polulale rjave veverice.
Od silovitega krohota je padla z drevesa celo gospa sraka,
da je imela polno rit listov in maka.

Nežna škratica Vrtavka se je rada vrtela,
čeprav se je pogosto v kak zid zaletela.
Tako nerodno je plesala,
da je vsaj trikrat na teden na ubogem potolčenem nosu pristala.

Okrogla gospodična Špegi je otrokom delila špagete,
brez vsega, z omako, s sirom, sveže ali pogrete.
Imela jih je v vsakem žepu in laseh,
lezli so ji iz ušes in ust, vlekla jih je celo za sabo – po tleh.

Mali možiček Fotko pa ni šel nikamor brez fotoaparata.
Takega, ki je slikal in snemal, dal mu ga je sam slavni režiser – stari ata.
Fotko je snemal in slikal vse škratkinje in možičke,
stare in mlade, dojenčke in stričke.

In vse – **PRAV VSE** – je objavil na spletu,
v hipu se je razširilo po VSEM širnem svetu!
In **PRAV VSI** ljudje so videli:
kako ima Pepe polna ušesa repe,
kako Smrdec spusti glasen prdec,
kako se Špegi med paradižnikovimi špageti kotali,
kako Spaka od smeha trebuh boli
in kako se Vrtavka prav nerodno vrti in čudno drži.

Posnetek je postal prava uspešnica,
strašansko gledana smešnica.

Od blizu in od daleč preplezali so gričke,
da bi videli te čudne skratice in možičke.
Vsi so se norčevali,
vsi so se jim smejali.
Škratice in možički pa so si samo želeli nekam daleč uiti,
se pod mehki mah skriti.
Čas zavrteti nazaj, nazaj,
ko njihov dom je bil še pravi raj.

Ko druga bitja v njih niso videla samo, kako so nerodni, packasti ali bolni,
ampak dobri po srcu in življenja polni!
Ko niso bili samo čudne spake, pa saj ima vsak kakšne manjše napake!

Toda vrnitve nazaj ni bilo,
škratki so bili potrti, žalostni, bilo je res hudo.
Tudi Fotko se je nekam skril,
in se hudo sekiral,
ko je ugotovil, kaj je nespametno storil
in kaj je zrežiral.

Leta in leta so potrebovali,
da spet so z drugimi prave vezi stkali.
Škratice in možički so se sčasoma malce pomirili,
čeprav na svojo sramoto niso nikdar čisto pozabili.

In čeprav je Fotko čez tri leta nov filmček posnel,
same dobre in lepe stvari iz njihove vasice zajel:
Pepeta, ki dela zavzeto,
Smrdca, ki sosedu oskrbuje ranjeno peto,
Spaka, ki se s starčkom na ves glas smeje,
Špegi, ki otrokom špagete greje,
Vrtavko, ki ji je ravno uspel super trik,
celo vasico, ki je bila prekrasna in šik.

In čeprav so spet...
od blizu in od daleč preplezali gričke,
da bi videli te prijazne in ljubeče škratice in možičke.
So se škratice in možički mičkeno manj smejali,
v srčki pa za vedno malo žalostni ostali.

1.2.3.2. Izmišljeni obrazec za registracijo

www.faceinfaconi.com

Vzdevek*:

Ime in priimek*:

Letnica rojstva*:

Naslov:

Telefonska številka*:

Številka kreditne kartice:

e-naslov*:

Geslo za mojo e-pošto:

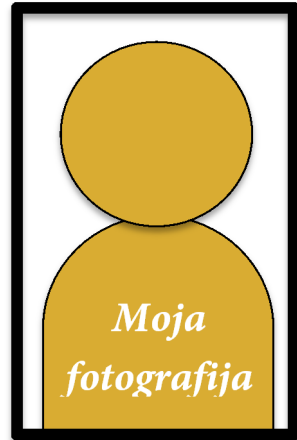
Moja šola*:

Moji krožki:

Kam rad grem:

Hobiji in kaj me zanima:

Kaj delajo moji starši:



* obvezno izpolniti

1.2.3.3. Zlata pravila faconk in faconov na internetu



1. Ne izdajaj osebnih podatkov: npr. imena in priimka, datuma rojstva, telefonske številke, e-pošte in gesla.
2. Ne posreduj podatkov o svoji družini, prijateljih ali šoli.
3. Bodi vedno vljuden.
4. Ne objavlaj čudnih, neprimernih posnetkov.
5. Zapomni si: kar je na spletu, ostane za vedno na spletu!
6. Če se ti zdi kdaj kakšna stvar na internetu čudna, takoj povej staršem.
7. Ne govori in ne dobivaj se z neznanci, ne pošiljaj jim svojih fotografij.

2. NAČRT UČNE URE 2: KDO ŽELI VAŠE OSEBNE PODATKE?

Małgorzata SZYSZKO in Katarzyna WIĄCZEK

2.1. UVOD

Zadnja leta smo priče hitremu razvoju informacijske in komunikacijske tehnologije. Internet ponuja številne storitve, ki jih mladi, pogosto nepremišljeno, uporabljajo za deljenje informacij o sebi. V virtualnem svetu je zaradi tega brez težav mogoče pridobiti veliko podatkov o njih in posledično ugotoviti, kdo so. To gotovo lahko predstavlja grožnjo za varstvo njihovih osebnih podatkov in zasebnosti.

Učitelji smo to spremembo opazili in prepričani smo, da so potrebni ukrepi, ki bodo zaščitili učence. Gre za velik izziv, tudi zato, ker vprašanja, povezana z varstvom osebnih podatkov in zasebnostjo predstavljajo novo področje za nas – učitelje. Zato je zelo koristno, da številne ustanove, npr. GIODO in fundacija Panoptykon, izvajajo različne oblike izobraževanja in obveščanja ter da lahko računamo na njihovo podporo in sodelovanje.

Na podlagi gradiva, ki so ga pripravile prej omenjene institucije, ob opiranju na lastne izkušnje s pedagoškim delom in na znanje o različnih metodah in oblikah dela z učenci ter z uporabo zanimivih učnih pripomočkov, se želimo lotiti izobraževanja mladih o varstvu osebnih podatkov in zasebnosti. Učencem in dijakom lahko ponudimo natečaje s tega področja, pa tudi srečanja s strokovnjaki. Vendar se zdi najbolj učinkovit pristop ta, da kompleksne vsebine v zvezi z varstvom osebnih podatkov celim razredom ali posameznim skupinam predstavimo v obliki učnih ur.

Tako smo se učitelji šole Marshal Józef Piłsudski št. 119 v Varšavi (*Gimnazjum nr 119 im. Marszałka Józefa Piłsudskiego w Warszawie*), odločili, da pripravimo scenarij, ki ga je mogoče izvesti v okviru različnih učnih ur in kjer je mogoče vsebino prilagajati med učnimi urami. Pri tem predpostavljamo, da imajo učenci že nekaj osnovnega znanja o varstvu osebnih podatkov in zasebnosti, ki so ga pridobili med preteklim izobraževanjem.

Učenci lahko dejavno sodelujejo pri izvedbi vsebine. Načrt učne ure predvideva, da delo poteka v skupinah in da učitelj predhodno pripravi gradivo. Nato sledi

predstavitev rezultatov skupinskega dela. Naloge posameznih skupin so neposredno povezane z vsebino predstavitve in z razpravo, ki naj bi se nato razvila v razredu.

Na svoji šoli smo tak scenarij izvedli v različnih oblikah učnih ur: v okviru učne ure iz računalništva za učence prvega razreda, v okviru razredne ure za učence drugega razreda in v okviru ure angleščine za zahtevnejšo skupino učencev tretjega razreda. Takšna raznolikost sledi domnevi, da imajo učenci različnih razredov različno visoko raven znanja o varstvu osebnih podatkov in o zasebnosti. Zaradi tega so pristopi k obravnavani tematiki zastavljeni različno zahtevno.

Scenarij omogoča učiteljem, da dosežejo zastavljene cilje. Vendar se je treba za delo dobro pripraviti in prilagoditi obseg vsebine posameznim skupinam. Zaradi tega se učne ure zdijo učencem zanimive, spodbujajo njihovo ustvarjalnost, kar je razvidno iz samega dela v skupini, sodelovanja v razpravah in prostovoljnega prevzemanja domačih nalog.

2.2. NAČRT UČNE URE

2.2.1. Opis

Ciljni razredi: učenci prvega, drugega in tretjega razreda druge stopnje osnovne šole (poljski izobraževalni sistem).

Vrste učnih ur: razredna ura, računalništvo, angleščina.

Splošni cilji: Seznaniti mlade s tem, zakaj je varstvo osebnih podatkov tako pomembno. Učenci se bodo naučili, kdo so upravljavci, ki želijo pridobiti njihove osebne podatke, pa tudi kakšna načela morajo ti pri tem spoštovati.

Specifični cilji:

Učenci naj:

- se naučijo, zakaj institucije, organizacije in podjetja zbirajo, hranijo in uporabljajo osebne podatke;
- spoznajo dolžnosti upravljavcev osebnih podatkov;
- se naučijo, da naj svoje osebne podatke razkrivajo premišljeno in da se je treba seznaniti s tem, za kakšne namene upravljavci osebnih podatkov obdelujejo naše osebne podatke.

Učne metode:

- učiteljeva navodila, izročki za učence, skupinsko delo;
- prikaz multimedijske predstavitve, ki jo pripravi učitelj;
- pogovori, razprave;
- uporaba informacijskih orodij.

Oblike dela:

- pritegniti pozornost učencev k snovi, ki jo posreduje učitelj;
- skupinsko delo na podlagi učiteljevih navodil in gradiva, ki ga pripravi, ter uporaba računalnika, ki naj bo povezan na internet;
- ogled multimedijske predstavitve;
- pogovori, razprave o ključnih vprašanjih in primerih v zvezi s snovjo učne ure.

Učni pripomočki in gradivo:

- prostorska oprema – mize, ki naj bodo pripravljene za skupinsko delo;
- mape z gradivom, ki naj vsebuje naloge za posamezne skupine;
- računalnik z dostopom do interneta, projektor;
- listi A4 papirja, flomastri, kemični svinčniki;
- magnetna tabla (lahko tudi plutovinasta ali celo kartonska tabla).

Ključne besede: osebni podatki, zbiranje podatkov, upravljavec osebnih podatkov, obdelava, varnost.

2.2.2. Potek učne ure

2.2.2.1. Uvod (osnovno znanje)

Priča smo zelo hitremu razvoju informacijske in komunikacijske tehnologije, ki prinaša številne koristi. V tem procesu nastajajo obsežne zbirke podatkov, ki jih obdelujejo različni subjekti. Obseg in hitrost procesa obdelave podatkov nas postavljata pred izziv, kako zagotoviti ustrezno varovanja razkritih osebnih podatkov.

Nenadzorovana uporaba osebnih podatkov s strani institucij in podjetij lahko ljudem povzroča številne težave. To velja še posebej v primerih, ko gre za obdelavo osebnih podatkov mladoletnih. Do tega pogosto prihaja zaradi nepoznavanja problematike oziroma zaradi pomanjkanja znanja o tem, kako ravnati, da bi varovali svojo zasebnost. Na podlagi znanja, izkušenj in gradiva, ki ga pripravljajo institucije s področja varstva osebnih podatkov, lahko učitelji

pripravimo zanimive učne ure. Ob uporabi ustreznih pedagoških metod lahko mlade poučimo o tem, zakaj sta varstvo osebnih podatkov in zasebnost tako pomembna.

Med pripravo učne ure s tematskim naslovom *Kdo želi vaše osebne podatke?* domnevamo, da učenci že imajo osnovno znanje o osebnih podatkih in o zasebnosti. V vsakem primeru ponovitev te snovi predstavlja dobro podlago za uvajanje novih vsebin.

2.2.2.1.1. DEJAVNOSTI UČITELJA PRED UČNO URO

Za izvedbo takšne učne ure bi morali učitelji pazljivo pripraviti naslednje: naloge za učence v posameznih skupinah, opremo, ki je potrebna za izvedbo teh nalog, predstavitev teme *Kdo želi vaše osebne podatke?* in predvideno domačo nalogo.

Takoj pred začetkom učne ure je treba pripraviti učilnico – tri mize za skupinsko delo in ostale predmete, ki so potrebni, da učenci izvedejo naloge.

2.2.2.1.2. ZAPOREDNE FAZE UČNE URE

1. Začetek učne ure – uvodni pozdrav, pojasnila o obliki dela, razdelitev učencev v skupine, dodelitev nalog – 5 minut;
2. učenci izvedejo svoje naloge – 10 minut;
3. učenci predstavijo svoje naloge in rezultate skupnega dela – 5 minut;
4. predstavitev in pogovori ter razprave pod neposrednim vodstvom učitelja v zvezi s temo *Kdo želi naše podatke?* – 20 minut;
5. povzetek učne ure, razprava o domači nalogi – 5 minut.

2.2.2.1.3. PODROBEN OPIS ZAPOREDNIH STOPENJ UČNE URE

1. Začetek učne ure – učitelj učence povabi v učilnico, kjer jim pojasni, da bodo delali v skupinah. Pozove jih, naj se razdelijo v tri skupine:
 - učenci, ki radi pripravljajo novičke in križanke, se pridružijo skupini 1. Člani skupine dobijo magnetno tablo, na katero pritrdijo listke, ki se navezujejo na določeno tematiko osebnih podatkov, primere osebnih podatkov in upravljalcev, ki jim prek spleta posredujemo svoje osebne podatke.

- Učenci, ki so spretni v iskanju informacij prek spleta, se pridružijo skupini 2, ki dobi računalnik z dostopom do interneta in projektor.
 - Učenci, ki radi rišejo in so spretni pri umetnosti, se pridružijo skupini 3. Učencem učitelj razdeli liste papirja, flomastre in kemične svinčnike, ki so potrebni za pripravo risb.
2. Učenci izvedejo svoje naloge. Za to imajo približno 10 minut časa. Učitelj nadzira delo učencev, preverja, ali so razumeli svoje naloge, nadzira napredek in jih opozori na čas, ki je namenjen izvedbi posameznih nalog. Če je treba, učitelj tudi disciplinira učence.
 3. Po izvedbi nalog vodja skupine predstavi naloge in rezultate skupinskega dela svoje skupine.
 4. Po koncu skupinskega dela učitelj učence pozove, naj se zberejo okoli zaslona, na katerem bo multimedijška predstavitev.

Naslov teme učne ure je: *Kdo želi vaše osebne podatke?* Predstavitvi sledi razprava, tako da imajo učenci možnost povedati svoje mnenje ali podati svoja pojasnila, še preden se soočijo s konkretnimi vprašanji ali ključnimi besedami. Potek razprave in vprašanj naj vsebinsko sledi nalogam, ki so jih izvedli učenci.

Posebna pozornost naj bo namenjena tistim vidikom snovi v predstavitvi, ki se neposredno nanašajo na specifične cilje, ki jih želimo v okviru učne ure doseči. Na primer:

- učencem je treba odgovoriti na vprašanja, zakaj institucije, organizacije in podjetja zbirajo, hranijo in uporabljajo naše osebne podatke;
 - treba je pojasniti dolžnosti upravljavcev osebnih podatkov;
 - Učence je treba naučiti, da svoje osebne podatke razkrivajo (če že) premišljeno in da se predhodno seznanijo z izjavo o zasebnosti upravljavca osebnih podatkov in z varnostnimi ukrepi, ki jih mora ta zagotoviti.
5. Zaključek učne ure – tukaj povzamemo vsebino učne ure in poudarimo, da je varstvo osebnih podatkov danes zelo pomembno. Zastavimo nekaj vprašanj, da se prepričamo, če so se učenci osvojili nove informacije in utrdili prejšnje znanje.

Določimo domačo nalogo. Učencem se zahvalimo za sodelovanje v učni uri.

Domača naloga:

- Domača naloga (učna ura z razrednim učiteljem): učenci se morajo s starši pogovoriti o izzivih, ki so bili predstavljeni pri učni uri, na primer o tem *kdo želi naše osebne podatke?*
- Domača naloga (računalništvo):
 - Učenci se morajo pogovoriti s starši o izzivih, ki so bili predstavljeni pri učni uri, na primer o tem *Kdo želi naše osebne podatke?*
 - Učenci morajo narediti avatarja iz slike, skladno z navodili učitelja – dodatna naloga za prostovoljce.
- Domača naloga (angleščina): zapisati nove besede in tvoriti stavke z njimi.

Ocenjevanje: znanje učencev preverjamo tako sproti kot na koncu učne ure. Predstavitev, ki predstavlja osnovo za pogovor in za razpravo, je prikazana tako, da omogoča učencem, da spregovorijo, preden se pojavi vprašanje ali ključna beseda. Opazujemo odzive učencev. Na koncu učne ure jih vprašamo, katere informacije so bile zanje nove, prav tako jim zastavimo nekaj vprašanj, da ugotovimo, kaj so si zapomnili.

Ostale opombe: Razvit scenarij je precej univerzalen in se lahko uporabi pri različnih učnih urah, ki jih izvajajo različni učitelji. Prav tako je mogoče vnesti element skrivnosti, tako da učitelj ne pove, katero temo bo obravnaval, pač pa učenci to sami odkrivajo po nalogah v skupinah. Za tekoče delo v skupinah morajo biti naloge za učence dobro pripravljene, prav tako morajo učenci dobiti vse ustrezno gradivo. Za skupino, ki razporeja listke na tabli, je magnetna tabla najbolj koristen pripomoček. Če nimate takšne table, zadošča tudi tabla iz plutovine, ki omogoča pritrdjevanje listkov z risalnimi žeblički, oziroma kartonasta tabla, na katero prilepimo koščke papirja z ustreznimi informacijami. Učna ura o varstvu osebnih podatkov in zasebnosti je ena številnih učnih ur, ki jih je mogoče uresničiti z obogatitvijo jedrnega učnega načrta, kar pomeni, da je takšno učno uro pomembno pripraviti z vso odgovornostjo in na zanimiv način.

3. NAČRT UČNE URE 3: SPLETNE NEVARNOSTI

Eszter KESZY-HARMATH

3.1. PRIHODNOST SE JE ZAČELA...

V zadnjih letih smo pedagogi jasno začutili, da umetnost poučevanja ne potrebuje zgolj običajne prenove, pač pa prenovo, ki se mora močno opirati na tehnologijo. Današnji učenci, t. i. Z generacija, so se rodili v svet informacijske tehnologije. Pripravljeni so biti pozorni in se učiti le, če lahko uporabljajo orodja informacijske tehnologije za pridobivanje novih informacij. Žal mladi danes živijo v takšnem svetu tudi zunaj učilnic, zato je velik del njihovega prostega časa zapolnjen s telefoni, računalniki in internetom. Ne vedo, da je poleg prednosti, ki jih prinaša tehnologija, v virtualnem svetu skritih tudi veliko nevarnosti. Mi, manj mladi, se lahko znajdemo v težavah, ko želimo uporabiti nove aplikacije. Vendar ob tem vemo, da danes sicer vsi mladi uporabljajo nove komunikacijske platforme (naj bo to Facebook, Twitter ali Skype), vendar se ne zavedajo tveganj, na katera utegnejo naleteti. Zato je očitna potreba po ukrepanju, vendar učitelji morda ne vedo, kako in kje naj začnejo. Zato je bil seminar za učitelje v okviru projekta ARCADES, ki ga je gostil madžarski Nadzorni organ za varstvo osebnih podatkov in prost dostop do informacij (NAIH), v veliko pomoč pri iskanju ustreznih načinov, kako ukrepati. Dobili smo veliko koristnih informacij in napotkov, kako pokazati učencem, da postanejo zavedni uporabniki interneta.

Po seminarju sem se pogovorila s svojimi učenci v šoli *Karácsony Sándor Általános Iskola* v Budimpešti. Skupaj smo pripravili načrt učne ure. Učencem smo dodelili naloge in jim tako pomagali pri dvigu zavesti o tem, kakšne nevarnosti prežijo nanje na spletu in kakšne so rešitve. Učno uro je spremljalo osebje NAIH. Kasneje smo bili obveščeni, da bomo kot zmagovalci nacionalnega tekmovanja zastopali madžarsko šolo na zaključni konferenci projekta ARCADES.

Na udeležbi na zaključni konferenci smo spoznali ostale vrhunske ekipe, odkrili nove ideje in se seznanili z razvojem podobnih učnih ur na Poljskem in v Sloveniji. Poučili smo se, kako je mogoče to široko in barvito tematiko učinkovito prikazati na drugačen način, z osredotočenostjo na različne starostne skupine učencev. Od udeležencev in od predstavnikov NAIH smo se naučili veliko novih, zanimivih in koristnih reči v zvezi z varstvom osebnih podatkov.

Zaradi tega se jim zahvaljujemo za prijaznost. Prav tako se za prijaznost zahvaljujemo vsem tistim, ki so si prizadevali seznaniti nas z izzivi varstva osebnih podatkov in zasebnosti ter z rešitvami, ki nam zdaj omogočajo, da učence učimo previdnosti pri ravnanju z osebnimi podatki.

3.2. NAČRT UČNE URE

3.2.1. Opis

Ta načrt učne ure je bil razvit v okviru področja medijskih študij za majhno skupino učencev madžarskega osmega razreda. Glavni poudarki so namenjeni spletnim nevarnostim, vključno s sekstingom in spletnim nadlegovanjem. Priložen scenarij pokriva le del znanja o zasebnosti, ki bi moralo biti posredovano učencem. Vsaj sedem podobnih učnih ur bi bilo treba izvesti, da bi naslovili ostale nevarnosti na internetu ter druge vidike varstva osebnih podatkov.

Cilji in naloge učne ure				
razvoj veščin pomnjenja	razvoj vidnega zaznavanja, veščin pozornosti in koncentracije	poglobljanje naučenega znanja	širitev besednega zaklada	razvijanje interoperabilnosti
razvoj govornih veščin	razvoj razmišljanja	razvoj veščin nadzora	razvoj komunikacijskih veščin	razvoj veščin sodelovanja

3.2.1.1. Potek učne ure

Časovni okvir	Dejavnost	Opis dejavnosti	Metode	Učne oblike	Pripomočki
3 minute	Priprava ogrevanje	reševanje križank (pregled znanja definicij) Definicije, ki jih je treba rešiti: ikona, vzdevek, televizija, elektronski	razvijanje zmožnosti pomnjenja aktivacija obstoječega znanja	v parih	Priročnik

		podpis, usmerjevalnik, netiketa, e-pošta, troll. Rešitev je: INTERNET.			
--	--	---	--	--	--

2 minuti	Poprava	razprava	razlaga	frontalna oblika	neodvisna poprava
2 minuti	Razprava	Moto 21. stoletja bi lahko bil: <i>Bodimo zdravi in imejmo dovolj močan internetni signal!</i> - Kaj je pomen mota? - Se strinjate z njim?	razlaga	frontalna oblika	interaktivna tabla: projekcija
3 minute	grafično	Osrednji element grafike: INTERNET. Naloga: zapolnite prazna mesta z besedami, ki se nanašajo na INTERNET.	ustvarjanje miselnega vzorca, razlaga, proste asociacije	frontalna oblika	Tabla
3 minute	plakat	Interpretacija ilustracije <i>Confessional</i> , katere avtor je Pawel Kuczynski.	slika interpretacija, razprava	frontalna oblika	Slika
3 minute	avdio vizualni učinek	ogled videa <i>Wo ist Klaus?</i> (na voljo v različnih jezikih na): http://www.klicksafe.de/ueber-klicksafe/downloads/klicksafe-werbespots/download-wo-ist-klaus/ analiza videa o spletnih nevarnostih	razprava	frontalna oblika	Video
5 minut	pogovor	Naloga: opišite pomen naslednjih besed: pridobivanje zaupanja, troll, flaming, meme, seksting, spletno	vodenje razvijanje samoizražanja spodbujanje	frontalna oblika	Tabla

		nadlegovanje.	lastnih idej		
7 minut	prizor	Naloga: izvleci listek in izvedi zahtevan prizor.	dva situacijska prikaza pod učiteljevim neposrednim vodstvom v povezavi s temo spletnega nadlegovanja in kraje identitete	frontalna oblika	lističi
2 minuti	pripovedovanje nedokončane zgodbe	priporočena dejavnost ARCADES aktivnost, <i>Najbolj zasebne stvari</i>	Učitelj prebere zgodbo razredu.	frontalna oblika	interaktivna tabla, priročnik
10 minut	razprava	Vprašanja: <ul style="list-style-type: none"> - Kaj bi se lahko zgodilo? - Kako bi lahko deček in deklica preprečila situacijo? - Se lahko podobna zgodba zgodi v resničnem življenju? - Če ne, kakšne zgodbe si še lahko predstavljate? 	razprava, razlaga	frontalna oblika, samostojno delo	
5 minut	razprava s ciljem ozaveščanja s pomočjo uporabe interneta in razmišljanje o nevarnostih preden se odločimo.	Vprašanja: Kaj bi storili v tvegani ali v nevarni situaciji? Kje iskati pomoč? <ul style="list-style-type: none"> - starši, - odrasli, - organ za varstvo osebnih podatkov, - ombudsman, - telefon za klic v stiski - internetna točka za pomoč. 	izjava učitelja, razlaga, evaluacija	frontalna oblika	interaktivna tabela, priročnik

SLOVARČEK

Kraja identitete: izdajati se za nekoga drugega; pridobiti dovolj informacij o osebi, da se lahko pretvarjamo, da smo ta oseba.

Občutljivi osebni podatki: osebni podatki, ki potrebujejo posebno zaščito, npr. podatki o prepričanju posameznikov, njihovem zdravstvenem stanju, rasnem, narodnem in narodnostnem poreklu, spolnem življenju idr.

Osebni podatek: katerikoli podatek, ki se nanaša na posameznika, ne glede na obliko, v kateri je izražen; lahko gre za pisno informacijo, sliko, zvok, prstni odtis ipd.

Posameznik: oseba, na katero se osebni podatki nanašajo in ki ima glede teh podatkov tudi določene pravice.

Pravica do varstva osebnih podatkov: ta temeljna pravica dalje ljudem vrsto pravic glede njihovih osebnih podatkov, hkrati pa tistim, ki z osebnimi podatki razpolagajo, nalaga vrsto dolžnosti. Nadzor nad spoštovanjem pravil izvršuje organ za varstvo osebnih podatkov.

Pravica do zasebnosti: tradicionalno je poznana kot 'pravica, da nas pustijo pri miru'. V tej temeljni pravici je zajet širok nabor upravičenj, s katerimi se varuje zaupnost komunikacij, nedotakljivost stanovanja, družinskega življenja in osebnih podatkov. Na splošno lahko rečemo, da gre za pravico vsakogar, da živi svoje življenje svobodno in brez nepotrebnih posegov vanj.

Privolitev: prostovoljna, svobodna, izrecna in nedvoumna izjava posameznika, da se lahko njegovi osebni podatki obdelujejo za namen, ki ga je določil upravljavec osebnih podatkov.

Profiliranje: postopek zbiranja in analiziranja podatkov o posamezniku. Na podlagi zbranih podatkov so posamezniki razvrščeni v posamezne kategorije oz. profile na podlagi podobnih značilnosti, preferenc, aktivnosti. Na podlagi teh

zbranih informacij se lahko nadalje sklepa tudi na dodatne informacije o analiziranih posameznikih.

Ribarjenje podatkov: poskus pridobiti podatke, kot so denimo uporabniško ime, geslo, podatke kreditne kartice, na način (po navadi preko elektronske pošte), da pošiljatelj takšnega sporočila deluje kot zaupanja vredno podjetje ali posameznik.

Spletna identiteta: vtis, ki si ga lahko ustvarimo o osebi na podlagi informacij, ki so dostopne na spletu.

Spletno trpinčenje in nadlegovanje: škodljivo ravnanje, nadlegovanje, grožnje in trpinčenje nekoga z uporabo spleta, posebno, ko je takšno ravnanje storjeno namenoma in se ponavlja.

Upravljalci osebnih podatkov: organizacija, ki je odgovorna za obdelavo osebnih podatkov.

Vedénjsko oglaševanje: spletni oglas, ki temelji na predhodnem vedénju posameznika na spletu in ima zaradi zbranih podatkov o posamezniku več možnosti, da bo uspešen.

UPORABNI VIRI

Nadzorni organi za varstvo osebnih podatkov: če iščete več informacij o pravilih varstva osebnih podatkov v vaši državi ali vas morda zanima posebna tema, na tej povezavi http://ec.europa.eu/justice/data-protection/bodies/authorities/eu/index_en.htm najdete kontaktne podatke vseh organov glede na državo članico. Na spletnih straneh mnogih organov lahko najdete uporabna gradiva za otroke in mlade ter učitelje.

Informacijski pooblaščenec RS: nadzorni organ za varstvo osebnih podatkov v Sloveniji na svoji spletni strani objavlja mnoge smernice glede varstva osebnih podatkov, med drugim tudi mnogo materiala, namenjenega mladim in sodobnim tehnologijam. Je tudi član sveta Centra za varnejši internet Slovenije. <https://www.ip-rs.si/>

Centri varne rabe interneta: če potrebujete pomoč glede varnosti na internetu za mladoletne, so centri varne rabe pravi naslov. Običajno vključujejo aktivnosti ozaveščanja in telefonske številke za klice v stiski. Več informacij in kontaktne podatke lahko najdete na: <https://www.betterinternetforkids.eu/web/portal/policy/unsafe-inhope>.

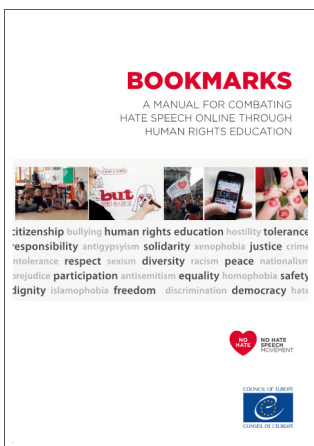
Safe.si, točka ozaveščanja o varni rabi interneta in mobilnih naprav za otroke, najstnike, starše in učitelje: <http://safe.si/>

Spletno oko, točka za prijavo sovražnega govora in posnetkov spolnih zlorab otrok na internet: <http://safe.si/spletno-oko>.

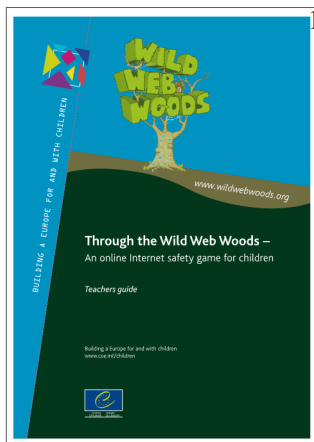
Listina Evropske unije o temeljnih pravicah: našteva vse temeljne pravice, ki jih zagotavlja pravo EU. V 7. členu določa, da ima vsak pravico do spoštovanja svojega zasebnega in družinskega življenja, doma in korespondence. 8. člen pa določa, da ima vsak pravico do varstva osebnih podatkov, ki se nanašajo nanj. Celotno besedilo je dostopno v vseh uradnih evropskih jezikih na: <http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A12012P%2FTXT>.



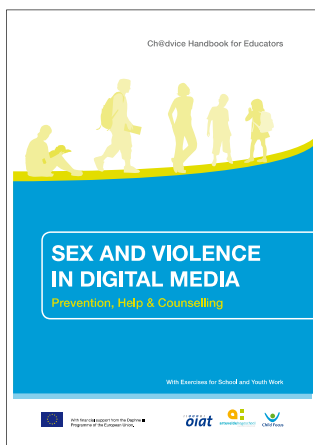
Priročnik o evropski zakonodaji s področja varstva osebnih podatkov: če vas zanima več o pravu varstva osebnih podatkov na ravni EU in na ravni Sveta Evrope, je odlična začetna točka omenjeni priročnik, ki sta ga leta 2014 skupaj izdala Svet Evrope in Agencija za temeljne pravice (FRA). Je brezplačen in dostopen v več evropskih in nekaj ne-evropskih jezikih na: <http://fra.europa.eu/en/publication/2014/handbook-european-data-protection-law>.



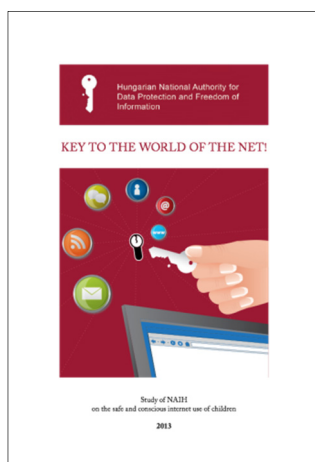
Zaznamki: s podnaslovom *Navodila za boj proti spletnemu sovražnemu govoru z izobraževanjem o človekovih pravicah* so gradivo, ki je namenjeno učiteljem, ki želijo o sovražnem govoru na spletu poučevati z vidika človekovih pravic, znotraj ali zunaj sistema izobraževanja. Oblikovan je za slušatelje stare od 13 do 18 let, aktivnosti pa so lahko prilagojene tudi drugim starostnim skupinam. Angleška in francoska verzija sta dostopni preko Sveta Evrope, druge jezikovne različice pa preko nacionalnih kontaktnih točk. Več informacij najdete na: <http://www.nohate.speechmovement.org/bookmarks>.



Skozi spletni pragozd (Through the Wild Web Woods): spletna igrica, ki jo je podprl Svet Evrope, za pomoč otrokom, da se varno gibajo po spletu. Dostopna je v več kot 20 jezikih in podprta s spremljevalnim vodičem: www.wildwebwoods.org.



Spolnost in nasilje v digitalnih medijih: priročnik za učitelje z uporabnimi informacijami o medijskem nasilju in fenomenu spletnega nadlegovanja, sextinga in groominga. Pripravil ga je Avstrijski inštitut za uporabne telekomunikacije (OIAT) in je dostopen v več jezikih na povezavi: <https://www.saferinternet.at/chadvice/>.



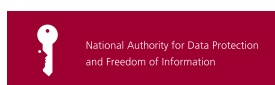
Ključ do sveta spleta! Je študija 'o varni in zavedni rabi spleta za otroke', ki jo je pripravil madžarski Nadzorni organ za varstvo osebnih podatkov in prost dostop do informacij (NAIH) s ciljem spodbujanja pravno 'zavedne rabe interneta pri otrocih, ki je osnovana na varovanju temeljnih pravic'. Več informacij in različne jezikovne različice so dostopne na tej povezavi: <http://www.naih.hu/adatvedelemr-l-fiataloknak-kulcs-a-net-vilagahoz--projekt.html>.

Priročnik vsebuje praktične nasvete in orodja za poučevanje otrok in najstnikov v šolah po celotni Evropi o zasebnosti in varstvu osebnih podatkov. Jasno in temeljito obravnava teme, kot so pravice posameznikov, varnost na spletu, digitalna identiteta, vedenjsko oglaševanje, spletno trpinčenje in nadlegovanje ter nadzor s strani staršev. Učitelji in strokovnjaki s področja izobraževanja bodo v priročniku našli izčrpno razlago glavnih poudarkov teh tematik pa tudi ideje za pogovor, primere praktičnih vaj in uporabnih nasvetov, prilagojenih različnim starostnim skupinam in razredom, ter primere učnih ur, ki so zmagale na natečaju. Strokovnjake za zasebnost in varstvo osebnih podatkov ter nadzorne organe za varstvo osebnih podatkov pa bodo zanimali novi pogledi na izobraževanje o zasebnosti in na to, kako med mladoletniki zvišati raven zavedanja o tej tematiki. Vključeni so tudi Mini listina pravice do zasebnosti in varstva osebnih podatkov, slovar in seznam uporabnih virov.

Publikacija predstavlja prvi izčrpen priročnik take vrste z evropskim dosegom. Je rezultat sodelovanja pravnih strokovnjakov in nacionalnih organov za varstvo osebnih podatkov v projektu Vnašanja tematik varstva osebnih podatkov in zasebnosti v šole v Evropski uniji (projekt ARCADES), ki je bil sofinanciran s strani programa "Temeljne pravice in državljanstvo" Evropske unije. Priročnik je rezultat skupnih prizadevanj partnerjev pri projektu: poljskega Glavnega inšpektorja za varstvo osebnih podatkov (GIODO), Informacijskega pooblaščenca Republike Slovenije (IPRS), madžarskega Nacionalnega organa za varstvo osebnih podatkov in prost dostop do informacij (NAIH) ter Raziskovalne skupine skupine za pravo, znanost, tehnologijo in družbo (LSTS) z Vrije Universiteit Brussel (VUB).



Co-funded by
the European Union



ISBN 978-94-000-0770-3

