Culture of Polis

КУЛТУРА ПОЛИСА

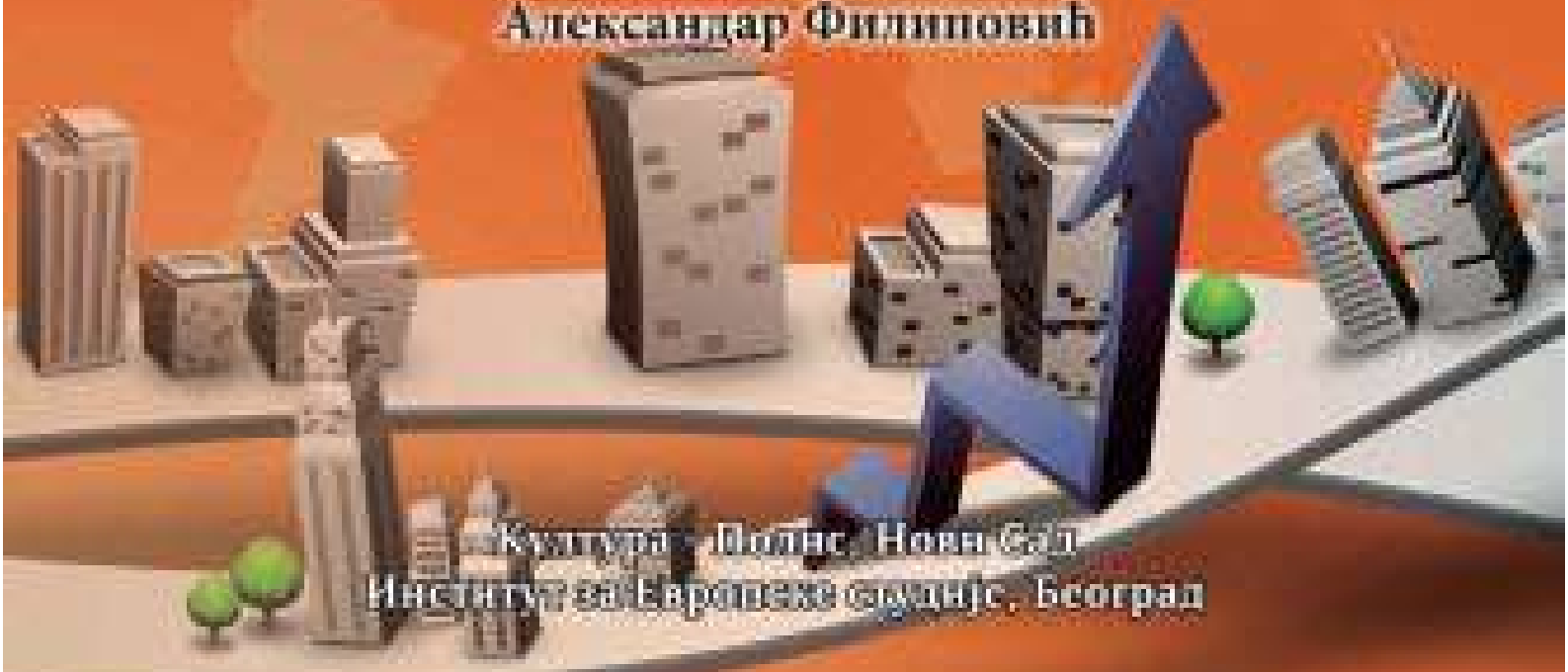
ISSN 0350-5588

Часопис за неговање демократске политичке културе
Journal for Nurturing of Democratic Political Culture

Година XVIII | посебно издање | 2018. година

ПЕРСПЕКТИВА УВОЂЕЊА БЕЗБЕДНОСНЕ КУЛТУРЕ У ОБРАЗОВНИ СИСТЕМ РЕПУБЛИКЕ СРБИЈЕ

приредили:
Жељко Бјелајац
Александар Филиповић



Култура полис, Нови Сад
Институт за европске студије, Београд

ЈЕЛЕНА СТОЈШИЋ ДАБЕТИЋ*
Правни факултет за привреду и правосуђе
Нови Сад

UDC: 316.774:351.74/.76
Прегледни рад
Примљен: 13.04.2021
Одобрен: 20.05.2021
Страна: 161–173
DOI: 10.51738/Kpolisa2021.18.1p.1.11

МОДЕРНИ И ПОСТМОДЕРНИ КОНЦЕПТ ДЕТИЊСТВА У СВЕТЛУ ОСИГУРАЊА БЕЗБЕДНОСТИ ДЕЦЕ У ДИГИТАЛНОМ ДРУШТВУ

Сажетак: Контекст овог рада јесте позиција деце у дигиталном окружењу, са посебним акцентом на ризике по безбедност деце који се у овом контексту јављају и како то креира модерне концепте детињства. Нове мобилне и интернет технологије стварају нове могућности за развој деце, али истовремено стварају низ нових ризика. То ствара оквир у коме друштвено- технолошки контекст утиче на креирање безбедносне политике, али и обрнуто. У раду се указује на неколико аспеката модерног, дигиталног друштва, који значајно мењају досадашње постулате на којима почива брига друштва о деци – посебан третман и садржај права детета као корисника дигиталне технологије, затим додатни механизми правног режима заштите података о личности којима се обезбеђује најбољи интерес детета, као и култура контроле као примарни наратив приликом креирања јавних политика безбедности деце у дигиталном окружењу. Без намере да се улази у појединости правних режима, рад истиче својеврсну јукстапозицију тежњи савременог друштва које жели да контролом постигне безбедност и истовремено омогући слободан развој деце у одрасле људе.

Кључне речи: деца, дигитално окружење, интернет, безбедност, култура контроле.

Уводна разматрања – деца у дигиталном друштву

Може се рећи да је савремено друштво - друштво безброј осветљених екрана. Ти екрани нису само дводимензионална представка традиционалних медијских садржаја, напротив – они су средство којим се остварује највећа међуповезаност људи и садржаја. Дигиталност и дигитализација су донеле

* j.stojsic.dabetic@pravni-fakultet.info

незапамћен низ промена, и то не само у технолошком смислу. Дигитална револуција захватила је све сегменте друштва, и изменила начин на који људска бића функционишу чак и на свакодневном нивоу, од социјализације до пословања, обухвативши и највећи део ствари између (Бјелајац и Филиповић 2021). Атрибут који се савременом друштву најчешће приписује јесте дигитално, што је последица високог степена улоге и значаја дигиталне технологије одн. информационо-комуникационих технологија у свакодневном животу. Савремено друштво се ослања на дигиталну технологију, дигитална технологија мења основне парадигме друштва, нема активности нити друштвених чиниоца који се у, мањој или већој мери не ослањају на различите видове дигиталне технологије и модалитете њене употребе. Деца, у смислу физичких лица која нису навршила 18 година старости, како их дефинише Конвенција Уједињених нација о правима детета, више су него активни корисници дигиталне технологије. Имајући у виду посебну одговорност које свако друштво и правни систем има у погледу осигурања најбољег интереса детета, и статуса деце као посебно рањиве друштвене групе, а у ширем контексту стварања и развоја дигиталног друштва, јављају се многа правна, друштвена, економска, безбедносна, морална и вредносна питања у вези са позицијом деце, посебно позицијом деце као корисника дигиталне технологије.

Терминолошки, појам детета подразумева лице које није навршило 18 година живота, а дигитално окружење (*digital environment*) подразумева информационе и комуникационе технологије, у смислу техничких средстава која преносе информације и преко којих се комуницира (компјутер, хардвер, софтвер у виду мобилних телефона, таблета, дигиталних камера и свих осталих "паметних" уређаја), укључујући и интернет и дигиталне медије. Управо је контекст овог рада позиција деце у дигиталном окружењу, са посебним акцентом на ризике по безбедност деце који се у овом контексту јављају. Нове мобилне и интернет технологије стварају нове могућности за развој деце, али истовремено стварају низ нових ризика. То ствара оквир у коме друштвено-технолошки контекст утиче на креирање безбедносне политике, али и обрнуто (Stepanovic 2014, 169). Примера ради, од 90-их година XX века Европска унија организује различите иницијативе и програме за постизање безбедности деце у дигиталном друштву, као што је Програми Европске комисије за безбеднији Интернет, Европска мрежа Центара за безбедан Интернет, као и европска политика превенције сајбер криминала.

Када се говори о односу деце према коришћењу интернета одн. других видова дигиталних комуникација, истиче се да деца данас живе у тзв. „међустварности" (*interreality*) као новом облику хибридне стварности, која је мешавина виртуалне и физичке стварности. Интеракције међу децом се данас одвијају и на виртуалној (онлајн/*online*) и на физичкој (офлајн/ *offline*) равни, путем различитих медија који се користе за комуникацију (Kokswijk, 2007, 40). Информационо - комуникационе технологије су важан инструмент у животу деце на који се ослања учење, социјализација, изражавање, инклузија и уживање права и слобода детета, али истовремено су пут ка угрожавању безбедности деце и инструменти потенцијалног насиља над децом. Коришћење интер-

нета је за децу начин попуњавања времена између дневних активности, а све више дневних редовних активности је пресељено у онлајн домен (нпр. гледање телевизије, па чак и школа). Данас је сасвим уобичајено да деца користе смарт телефоне за свакодневни приступ интернету, пре него бико које друго средство дигиталне комуникације, подаци показују да 57% деце своје телефоне на тај начин свакодневно користи (деца од 9-11 година). Осим тога, деца данас онлајн могу да гледају видео садржаје, посећују друштвене мреже (подаци показују да 10% деце дневно посећује друштвене мреже у Немачкој и чак 45% деце дневно у Србији), играње онлајн игрица и употреба за школски рад (Smahel et.al 2020, 25). Подаци показују да деца претежно користе интернет за комуникацију и забаву, а мање за остале садржаје. Такође, у већини европских земаља деца од 14-16 година старости троше два пута више времена на интернету у односу на децу од 9-11 година старости (Smahel et.al 2020, 19). Степен дигиталних вештина деце јесте основни предуслов за успешно коришћење интернета, али са више коришћења расту и вештине, а са растом вештина расту и ризици.

Савет Европе посматра права детета у дигиталном окружењу као један од приоритета, који подразумева стварање интернета који је безбедан, сигуран, отворен и доступан свима без дискриминације. Такође, дечија права, гарантована Конвенцијом УН о правима детета, и Европском конвенцијом за заштиту људских права и основних слобода, морају бити и остати заштићена независно од технолошког развоја. Комитет УН за права детета прокламује да сва деца морају имати безбедан приступ дигиталној технологији и дигиталним комуникацијама, и бити оснажена да у потпуности учествују, да се изразе, траже информације и уживају сва права гарантована корпусом дечијих људских права. Истовремено, безбедност деце у онлајн комуникацијама је данас редован предмет правног регулисања, јавних политика и јавних дебата – од кривичноправне до образовноправне, укључујући и контекст људских права и права детета. Не може се негирати корисност употребе интернета од стране деце, али не могу се негирати и све већи и опаснији ризици који из тога произилазе, те се као кључно питање поставља како заштити децу и омладину без да их превише ограничимо у слободном развоју? И није спорно да коришћење интернета децу поставља у позицију потенцијалних жртава, али и у позицију потенцијалних починилаца штетног понашања. Негативна искуства која су деца пријављивала, а са којима су се сусрела приликом коришћења интернета и других дигиталних комуникација јесте, између осталог, изложеност сексуалном садржају, агресивном садржају и другим облицима нежељеног садржаја, затим непристојан контакт, онлајн злостављање, дељење личних информација, урушавање угледа, примање вируса и онлајн реклама (Cortesi and Gasser 2017, 22-24).

Када се постави питање ко је одговоран за безбедност деце у онлајн комуникацијама, најчешћи одговори се односе на родитеље, затим на учитеље у смислу постизања дигиталне писмености у савременим условима развоја дигиталних технологија и модалитета комуникација, као и други друштвени чиниоци – невладине организације, тела који се баве заштитом деце, као и

привредни субјекти, који сносе део одговорности како директно у односима са децом као корисницима, тако и индиректно као подршка родитељима и учитељима. У онлајн комуникацији веома је тешко родитељима да уоче штетан контакт који њихово дете успостави. Родитељски надзор би се морао продужити и на онлајн комуникације њихове деце, што обухвата различите модалитете употребе интернета, у виду друштвених мрежа, онлајн игара, виртуелне реалности, форума, размене порука, web коришћење веб камера, итд, на различитим местима – од школе преко улице све до куће, тј. свуда где је телефон са њима. И врло често родитељи имају веома мали увид у то шта се дешава у онлајн свету своје деце, те не могу правовремено ни уочити ризике и реаговати. Меморандум уз Ланзароте конвенцију наводи забрињавајући феномен да се деца појављују као жртве сексуалних напада у онлајн састанцима одн. интеракцији са одраслима који се одвијају у сајбер простору – интернет причаоницама и сајтовима за игре. Широка доступност телефона овај вид недозвољеног понашања чини доступним и за доста млађу децу у односу на адолесценте, и тиме потребу за механизмима контроле чини већом.

Експериментално понашање, као и понашање које укључује одређене ризике је, како се стручњаци слажу, саставни део одрастања и емоционалног развоја деце, као и стварања сопственог идентитета, а све се то дешава кроз социјални контакт, где се данас интернет позиционира као основни виртуелни простор за стварање и одржавање социјалних контаката. А друге стране је реалност да све што се предузима онлајн је доступно свима и свуда, практично глобално, И сваки садржај може бити, и јесте доступан било којој претрази и умножавању. Врло често је веома тешко, скоро немогуће, потпуно уклонити садржај постављен на интернет, као што је сасвим лако креирати лажне профиле и пласирати различит садржај.

Правни оквир права детета у дигиталном окружењу – дете као активни чинилац у дигиталном окружењу

Када се као тема наметне друштвени аспект који има значајан утицај на децу, одн. где су деца значајан субјект друштвеног односа, очекује се да наратив постави оквирне смернице које се тичу права детета као посебног корпуса општих људских права. Општи оквир права детета у дигиталном окружењу чине прилично уједначене поставке у оквиру система Савета Европе и Европске уније, које ће у оквиру овог одељка бити представљене на општи начин.

Деца „излазе" на интернет чак и са 4 године, а пре поласка у школу готово да су овладала сурфовањем мрежом. Неколико сати дневно малишани су суочени са светом без икаквих ограничења, тако различитим од света у коме иначе живе. Тако наивни и невини лако постају плен интернет предатора. Предатори су интернетом добили брзи и анонимни приступ деци, место где могу да сакрију свој идентитет и лутају мрежом без ограничења. Интернет предатори су, у начелу, сексуални предатори. Обично их замишљамо као особе које лутају око школских игралишта и ту вребају своје потенцијалне жртве.

Међутим, стварност се променила. Данашњи сексуални предатори вребају жртве кријӯћи се иза рачунарског екрана, искориштавајӯћи претерану радозналост и лаковерност деце и анонимност коју нуди интернет. (Бјелајац и Филиповић 2020). Сваком детету мора бити омогућено да своја права и слободе ужива у дигиталном окружењу, одн. онлајн и офлајн, посебно право на живот и право на развој. Државе у своје јавне политике морају да уведу регулисање начина на које друштво користи дигиталне медије, а које има, или може да има последице по добробит деце. Основни принципи на којима почива систем заштите и остваривања права деце у дигиталном окружењу подразумевају, између осталог остварење набољег интереса детета, забрану дискриминације, право гласа детета (*right to be heard*), уважавање индивидуалних способности детета, примарну одговорност државе да осигура поштовање и остваривање права деце у дигиталном окружењу, право на слободан приступ и употребу дигиталне технологије, право на слободу изражавања и информисања, право на учешће, право на игру и окупљање и удруживање, право на приватност и заштиту података, дигиталну писменост, и право на заштиту и безбедност (Ad hoc Committee for the Rights of the Child (CAHENF)).

Остваривање најбољег интереса детета подразумева да се заштита детета постиже у равнотежи са правом на слободу изражавања и уз учешће детета у одлучивању о питањима која га се тичу. Забрана дискриминације не спречава усвајање посебних мера усмерених на децу која спадају у угрожене скупине, имајућӣ у виду да дигитално окружење може управо ту рањивост продубити, али истовремено је може и отклонити. У дигиталном окружењу деци мора бити омогућено да учествују у одлучивању, у складу са могућностима које имају према годинама и зрелости, као и да се слободно изразе користећи различите медије, док се истовремено мора осигурати ефективно учешће деце у развоју, имплементацији и оцени политика, механизама, пракси, технологија и ресурса који имају за циљ промоцију, заштиту и остварење њихових права у дигиталном окружењу. Држава и други чиниоци морају водити рачуна о способности деце, имајућӣ у виду децу са посебним потребама, инвалидитетом, и осигурати да усвојене политике одговарају њиховим потребама и развоју њихових потенцијала у дигиталном окружењу.

Ограничен или потпуно ускраћен приступ дигиталном окружењу лишава децу потпуног уживања својих загарантованих права. Државе имају обавезу да омогуће приступ уређајима, повезаности и садржајима, на сигуран и доступан начин. Посебно се мора водити рачуна о осетљивим групама деце, као што су деца у старатељским условима, деца лишена слободе или деца чији су родитељи лишени слободе, деца мигранти и деца у руралним подручјима. Државе морају остварити утицај на провајдере да осигурају да су њихове услуге доступне свој деци и на одговарајућ начин, посебно са асекта безбедности деце као корисника и садржаја одговарајућег деци као корисницима Државе морају поштовати улогу деце као креатора и преносиоца информација, али и деца морају бити свесна својих одговорности у том смислу, посебно у односу на права других. Дигитално окружење омогућава окупљање и удруживање кроз онлајн комуникацију и учешће одн. стварање и одржавање социјалних конта-

ката преко дигиталне мреже, као и одговарајуће начине за изражавање и креативност деце, уз поштовање њихових ауторских права. У тим активностима, деци се мора омогућити увид у своја права и начине заштите, на одговарајућ начин. Државе морају заштитити приватност деце, личне податке, онлајн углед и поверљивост преписке, како у односу на саму државу, тако и у односу на остале чиниоце. Обрада података која се односи на децу мора бити законита и правична, безбедна, са јасним пристанком субјекта на кога се подаци односе, у складу са законским гаранцијама. Посебно се мора водити рачуна о принципима приватности путем дизајна (*privacy by design*) и принципу подразумеване приватности (*privacy by default*). Обавештења о приватности и обради података морају бити таква да их деца могу разумети и у складу са тим дати свој информисан пристанак. Дигитална писменост мора бити део најранијег курикулума основног образовања, а подразумева развијање компетенција за коришћење дигиталне технологије, као и вештине креирања садржаја и критичког разумевања дигиталног окружења. Деца морају бити заштићена од ризика по њихово физичко и ментално здравље, посебно у односу на сексуалну експлоатацију и злостављање. Безбедност деце треба постићи тако да друга права, посебно она усмерена на развој деце, не буду сувише ограничена. Државе морају осигурати промоцију принципа безбедносног дизајна као водећег принципа у продукцији уређаја и сервиса усмерених на децу као кориснике, као и увести системе верификације узраста приликом коришћења уређаја и сервиса. Безбедност подразумева превенцију тешких кривичних дела која се дешавају у сајбер простору, као и превенцију пласирања незаконитог или штетног садржаја и материјала, укључујући материјал који представља злоупотребу деце.

Положај деце као субјеката правног оквира за заштиту приватности

Општа уредба Европске уније о заштити података о личности се посебно односи на заштиту деце и личних података у дигиталном свету. Рецитал 38 посебно истиче да су деца, као посебна категорија корисника дигиталне технологије, мање свесна ризика, последица и мера безбедности, као и својих права у оквиру процеса обраде личних података. Циљ система заштите предвиђеног Уредбом јесте посебна заштита од ре(употребе) личних података деце за потребе маркетинга и других комерцијалних услуга. У пракси, деца често нису способна да разумеју природу процеса обраде података, у смислу који подаци се обрађују, како се обрађују и ко је обрађивач. Надаље, нису увек способна да разумеју последице процеса обраде података, као и да разумеју свој правни положај у процесу обраде података, и тиме да ефективно користе своја права.

Члан 8 Уредбе је посвећен дистрибуцији овлашћења у вези са одлукама о законитој обради личних података о деци у руке родитеља или законских старатеља, у случајевима када деца нису у могућности да разумеју и нису довољно свесна да би била у стању да донесу самосталну одлуку, а према Уредби то су деца млађа од 16 година за чију обраду података се тражи пристанак ро-

дитеља. Државе могу поставити мању старосну границу, али не нижу од 13 година старости.

Ако је пристанак родитеља, одн. детета постављен као примарна линија одбране безбедности деце у дигиталном друштву, онда све слабости правног концепта пристанка се односе и на услов пристанка родитеља за обраду података о детету. Наиме, пристанак подразумева да путем давања пристанка успостављамо контролу над обрадом својих личних података, одн. да имамо стварну могућност избора и разумемо праксу обраде података од стране обрађивача. Правно гледано, субјект који учествује у трансакцији пристанка одн. давању пристанка тј. давалац пристанка мора имати довољан ниво способности за расуђивање и довољно иннформација, посебно о последицама давања пристанка. То децу и лица са менталним поремећајима чине неспособним за давање информисаног пристанка као правно ваљаног пристанка (Custers et.al 2013, 438). У пракси, уколико желимо да се пријавимо за онлајн услуге или да користимо апликације, једина могућност јесте да пристанемо на политику приватности која је предуслов коришћења. Једине опције које се нуде том приликом кориснику јесу "прихватам" или "не прихватам". Надаље, врло често корисници уопште не читају политике приватности, или их читају али не разумеју, а није мали ни број апликација у којима уопште није истакнута политика приватности (Schermer and Custers and Van der Hof 2014, 6).

Деца испоод 13 година морају имати пристанак родитеља за коришћење сервиса, чак и када су ти сервиси, услуге или апликације бесплатни. И пристанак родитеља мора бити проверљив. Проверљивост родитељског пристанка подразумева да се морају предузети разумни напори од стране пружаоца услуге одн. обрађивача података да осигура да је заиста родитељ тај који је дао пристанак, а на нивоу праксе се нису установили посебно поуздани механизми за такву проверу.

У пракси, давање детету у руке могућности да даје пристанак је проблематично на више нивоа, али са друге стране, инсистирање на пристанку родитеља доводи до стварања тензије између деце и родитеља у погледу очекивања поштовања приватности. Друштвене мреже, поред простора за комуникацију са вршњацима, омогућавају простор у коме млади очекују одређен степен приватности, ван родитељског надзора, И стриктно инсистирање на пристанку од стране родитеља може довести до надзора од стране родитеља који је неприхватљив. Захтев за родитељским пристанком у случају деце млађе од 13 одн. 16 година може негативно утицати на права еманципације и права учешћа те деце и креирању свог дигиталног окружења, довести до вишег нивоа родитељске контроле и тиме угрожавања права приватности деце, посебно код адолесцената којима је и онлајн приватни простор једнако битан као и физички приватан простор (без надзора родитеља). Неке онлајн услуге могу тим поступком бити онемогућене. Постизање безбедности у погледу обраде личних података деце може угрозити друга права и слободе деце.

Поред пристанка родитеља, Уредба предвиђа још неколико, општих, механизама који могу допринети безбедности деце, иако нису креирани посебно за заштиту деце – принципи приватности путем дизајна и подразумеване при-

ватности, као и процену утицаја обраде података. У контексту заштите деце подразумевају обавезу контролора и обрађивача података да воде рачуна о остваривању најбољег интереса детета приликом креирања својих оперативних, техничких и организационих процеса. принципи приватности путем дизајна и подразумеване приватности подразумевају да контролори имплементирају принципе заштите података у своје системе обраде података. Приватност путем дизајна подразумева да контролор примењује одговарајуће техничке и организационе мере (нпр. псеудонимизацију) које су креиране управо као израз принципа заштите података, као и да сам процес обраде података буде у складу са принципима заштите података

Принцип подразумеване приватности подразумева да контролори примењују одговарајуће техничке и организационе мере које осигуравају да се обрађују само лични подаци који су неопходни за конкретну обраду у питању. Ова два принципа су, у пракси, више везана за технолошки дизајн, пре него за организационе мере, у смислу интерне политике и праксе (Van der Hof and Lievens 2017, 3-7). Имајући у виду висок степен рањивости деце као друштвене групе и корисника дигиталне технологије, оправдан је посебан третман примене принципа приватности путем дизајна и принципа подразумеване приватности када се ради о системима у којима се обрађују подаци деце, као што су образовно-административни системи и системи бриге о деци.

Надаље, у Уредби се изричито истиче потреба заштите деце у вези са транспарентношћу праксе обраде података, што у пракси подразумева да подаци о процесу обраде података морају бити креирани у складу са перцепцијом деце, њиховим искуством и очекивањима, и посебно бити прилагођени различитим годиштима деце која приступају таквим садржајима, истовремено имајући у виду степен разумевања који деца могу да имају о дигиталној економији и уопште дигиталном окружењу. Такође, препорука је да се профилисање, као последица обраде података, не примењује уколико подаци указују да је корисник дете одн. лице испод 18 година старости. У вези са правом да се буде заборављен, стицањем пунолетства, субјекти који су обрађивали податке лица које је тада било малолетно, морају прибавити нову сагласност за даљу обраду података или у случају ускраћивања сагласности уклонити те податке.

Уредба, такође, утврђује обавезу да контролор процени утицај процеса обраде података који могу резултирати високим ризиком по права и слободе лица чији се подаци обрађују, И то пре саме обраде података. Будући да се деца сматрају посебно рањивом групом, то указује на потребу вршења процене увек када се ради о подацима деце.

У случају видео-надзора у школама, а везано за гаранције заштите права личности, школа јесте руковалац подацима које прикупља, држи, обрађује и користи, при чему може прикупљати само податке на које је законом или пристанком лица чије податке прикупља овлашћена, за законом одн. личним овлашћењем прописане сврхе, у складу са принципима тачности података, сврсисходности обраде и сразмерности обраде. Дакле, обрада података о личности ученика спаде у општи оквир заштите података о личности.

У школама деца, у својству ученика, могу бити предмет обраде података путем видео-надзора јавног простора, који обухвата простор испред школе, улаз у школу или приступ службеним просторијама, ходнике, а у циљу постизања безбедности ученика. Из предмета видео-надзора искључени су простори где корисници очекују већи степен приватности – тоалети, свлачионице, простор за одмор, итд. Видео-надзор се у пракси стручних тела за заштиту података о личности, сматра последњим средством које се има применити у изузетним случајевима, када се сврха безбедности не може постићи блажим средствима. У суштини, предмет видео надзора морају бити простори где се мора заштити безбедност, али безбедност може, и често јесте, више угрожена у оквиру простора који су искључени из покривености видео надзором, у чему ни школе нису изузетак.

Сврха обраде података о ученицима, у контексту видео-надзора у школама, јесте безбедност, али се мора водити рачуна на које све, мање инвазивне начине, и у складу са гаранцијама права на приватност и људско достојанство, се та сврха може постићи у оквиру боравка деце у школи, посебно у оквиру просторија где стално бораве и ученици и наставно особље (Повереник за информације од јавног значаја и заштиту података о личности (ПИЈЗЗПЛ) 2019, 33-34).

Деца и млади у својим активностима не могу избећи тренд надзирања у савременом друштву. Када се ради о надзору, две су стране: контрола и брига. Надзор може идентификовати неприхватљиво одн. штетно понашање или чак незаконито, али може и допринети заштити појединца. Било који облик надзора мора бити креиран тако да омогући индивидуални развој појединца.

Култура контроле као наратив у контексту употребе дигиталне технологије од стране деце

Током адолесценције деца би требало да достигну одређен степен независности и осећаја личне слободе, како у међусобним односима тако и у односима са родитељима, што се одвија кроз процес самосталног доношења одлука и ослањања на себе, уз остајућу потребу за родитељском подршком. И родитељска контрола током адолесценције би требало бити мањег обима.

Безбедност деце, било да се ради о употреби дигиталне технологије или другим контекстима, примарно је обавеза родитеља одн. старатеља, али када они то нису у могућности одн. када ризици превазилазе њихове могућности, јавне политике морају пружити заштиту деци. Када се ради о безбедности деце, као и у сваком другом контексту јавних политика која се односе на децу и омладину, важан циљ јесте постизање и поштовање саморазвоја и слободе деце као личности (Cortesi and Gasser 2017, 100-102). Аутономија личности током детињства и адолесцентског развоја доприноси израстању у одговорне и независне одрасле појединце, а неопходно током периода развоја јесте упуштање у експериментално понашање, упуштање у различите ризике и истраживање. Понашања која представљају превелик ризик се свакако морају онемогу-

ћити одн. исконтролисати, али истовремено се мора оставити довољан степен слободе како би се постигли циљеви развоја сваког детета (Van der Hoff, Koops 2011, 3-4).

Самостално успостављање и одржавање социјалних односа, у стварном свету и онлајн, је процес грешака и учења кроз који се стиче самосталност личности. У свему томе, посебно у сфери дигиталних комуникација, млади се често осећају непобедивим и недодирљивим, И често су несвесни ризика које њихово понашање носи. Такође, имају и мању могућност процене озбиљности ризика у које се упуштају, као и свест о последицама које њихово понашање може изазвати, како по њих, тако и по њихову ближу околину. Велика родитељска укљученост у начине коришћења интернета од стране деце доводи до већег степена безбедности, али ограничава искуство коиршћења интернета и развој дигиталних вештина и стицање искуства за избегавање штетних понашања. Оно што треба постићи јесте отворен дијалог између родитеља и деце, који резултира разумевањем онлајн искустава, вештина и поштовања права других ((Cortesi and Gasser 2017, 26-29) .

Јавне политике које се односе на употребу интернета од стране малолетника, су неопходне у савременом друштву, као додатни механизам надзору родитеља у погледу постизања безбедности деце. Ове политике се налазе између две крајности: културе контроле базиране на управљању ризицима и неговања аутономије деце која се развија управо кроз предузимање ризика. То условљава садржај политка у смеру подизања свести, стимулације самоконтроле, технолошких мера, одговорности, криминализације и правне регулативе. Страх од онога што се деци може десити, имајући у виду да су креатори јавних политика често управо људи који су и сами родитељи, природно условљава садржину политика ка све већој контроли која се жели успоставити над понашањем младих – од нивоа породице, преко школе па све до јавних политика.

Успостављање механизама који омогућавају контролу је данас друштвени тренд, што утиче на перцепцију до тада друштвено прихватљивих понашања као потенцијално опасних одн. увода у кривична дела (нпр. понуда вожње младој особи се данас сматра неприхватљивим понашањем које би млади требало да избегавају), школе се посматрају као својеврсне тврђаве, а ученици као популација потенцијалних жртава или преступника. Усвојен је тренд да што више активности младих треба да је под надзором. Јавне политике које се односе на дигиталну безбедност балансирају између слободе и контроле коришћења интернета од стране деце, док се политике спречавања сајбер криминалитета фокусирају често једнострано на контролу, са акцентом на кривичноправну заштиту, истовремено занемарујући важност учења кроз грешке у развоју личности (Van der Hoff, Koops 2011, 10). Једностраност кривичноправне заштите може крајње резултирати неефикасношћу, чак и контрапридуктивношћу у односу на одговор деце коју треба да заштити. У дигиталној комуникацији млади проналазе и ризике и могућности.

Прихватајући културу контроле, грађанско друштво постаје мање толерантно на независност и мање спремно на поверење, а то ствара савремени

оквир детињства данашњих генерација. Култура контроле се у највећој мери ослања на кривично право и оштрину предвиђених казни. Јавне политике се у овом домену креирају у оквирима ризика одн. уочавања, процене и контроле ризика, комбиновано са потребом избегавања ризика у циљу стварања "безбедне државе" у којој је одсуство стварне или претпостављене опасности највиша вредност која има предност над свим осталим циљевима.

Закључак

Данас су деца активни чиниоци у дигиталном окружењу, истовремено позиционирана као субјекти јавних политика усмерених на постизање безбедности деце у дигиталном окружењу. Данас је интернет незаобилазан елемент у одрастању, а то подразумева довољан степен медијске одн. дигиталне писмености одн. способности како родитеља одн. старатеља тако и деце. Веома је упитно колико деца, као конзументи дигиталне технологије, могу да разумеју своје лично и шире дигитално окружење. Постизање високог степена дигиталне писмености и свести о потреби и начинима безбедног понашања на интернету би требало да буде окосница јавних политика безбедности деце у дигиталном друштву. Такође, родитељи морају бити освешћени у погледу ризика који постоје за интеракције у дигиталном окружењу, како би их могли правовремено уочити и реаговати. Базирање јавних политика на култури контроле као наративу у контексту употребе дигиталне технологије од стране деце, указује на креирање нове парадигме детињства. Модерни концепт детињства се данас базира на потреби за постизањем равнотеже између слободе деце да се развију у одговорне и независне одрасле људе и потребе за контролом ризика који постоје у дигиталној комуникацији и дигиталном окружењу.

Литература

1. Бјелајац, Жељко Ђ. и Александар М. Филиповић. 2020. „Интернет и друштвене мреже као неограничени простор за концентрацију и мултиплицирано присуство педофила". У: „Педофилија – узроци и последице", ур. Жељко Ђ. Бјелајац и Александар М. Филиповић, посебно издање, *Култура полиса,* 29-40
2. Бјелајац, Жељко Ђ. и Александар М. Филиповић. 2021. „Флексибилност дигиталних медија за манипулативно деловање сексуалних предатора". *Култура полиса,* XVIII (44): 51-67, https://doi.org/10.51738/Kpolisa2021.18.1r.2.01.
3. Ad hoc Committee for the Rights of the Child (CAHENF), Drafting Group of Specialists on Children and the Digital Environment (CAHENF-IT). 2017. *Recommendation CM/REC(2018)x of the Committee of Ministers to Member States on Guidelines to promote, protect and fulfil children's rights in the digital environment*, Strasbourg.
4. Cortesi, S. and Gasser, U. (Eds.). 2015. Digitally connected: Global perspectives on youth and digital media, Berkman Center Research Publication No. 2015-6.
5. Custers, Bart and van der Hof, Simone and Schermer, Bart and Appleby-Arnold, Sandra and Brockdorff, Noellie. 2013. "Informed Consent in Social Media Use – The Gap between User Expectations and EU Personal Data Protection Law" *Script-ed: A Journal of Law and Technology* 10(4), 435-457.
6. Повереник за информације од јавног значаја и заштиту података о личности (ПИЈЗЗПЛ). 2019. *Заштита података о личности: ставови и мишљења Повереника*, Публикација бр. 4, Београд.
7. Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), Official Journal of the European Union, 2016/L119
8. Schermer, Bart and Custers, Bart and Van der Hof, Simone. 2014. „The Crisis of Consent: How Stronger Legal Protection may lead to Weaker Consent in Data Protection" *Ethics and Information Technology*, DOI: 10.1007/s10676-014-9343-8.
9. Smahel, D., Machackova, H., Mascheroni, G., Dedkova, L., Staksrud, E., Ólafsson, K., Livingstone, S., and Hasebrink, U. 2020. *EU Kids Online 2020: Survey results from 19 countries*, EU Kids Online. Doi: 10.21953/lse.47fdeqj01ofo.
10. Stepanovic, Ivana. 2014. „Modern technology and challenges to protection of the right to privacy" *Annals FLB – Belgrade Law Review*, Year LXII, No. 3, 167-178.
11. Van der Hof, Simone and Koops, Bert-Jaap. 2011. „Adolescents and Cybercrime: Navigating between Freedom and Control" *Policy & Internet*, Vol. 3, Iss. 2, Art. 4.

12. Van der Hof, Simone and Lievens, Eva. 2017. „The importance of privacy by design and data protection impact assessments in strengthening protection of children's personal data under the GDPR" Presented at the IALS Conference *Children and Digital Rights: Regulating Freedoms and Safeguards* (17 October 2017, London), To be published in: Communications Law 2018, Vol. 23, No. 1.
13. Van Kokswijk, J. 2007. *Digital Ego: Social and Legal Aspects of Virtual Identity*, Delft: Eburon Uitgeverij, ISBN-13: 978-9059722163 (navedeno prema Van der Hof, Simone and Koops, Bert-Jaap. 2011. „Adolescents and Cybercrime: Navigating between Freedom and Control" *Policy & Internet*, Vol. 3, Iss. 2, Art. 4).

JELENA STOJŠIĆ DABETIĆ*
Faculty of Law for Commerce and Judicary in Novi Sad
Novi Sad

Review work
Received: 13.04.2021
Approved: 20.05.2021
Page: 161–173

MODERN AND POSTMODERN CONCEPT OF CHILDHOOD IN THE LIGHT OF ENSURING CHILD SAFETY IN DIGITAL SOCIETY

Summary: The context of this paper is the position of children in the digital environment, with a special emphasis on the risks to child safety that arise in this context and how it creates modern concepts of childhood. New mobile and internet technologies create new opportunities for children's development, but at the same time create new risks. This creates a framework in which the socio-technological context influences the creation of security policy, and vice versa. The paper points out several aspects of modern, digital society, which significantly change the current postulates on which society's care for children is based - special treatment and content of children's human rights as users of digital technology, then additional mechanisms of legal regime of personal data protection, as well as the culture of control as the primary narrative in creating public policies for child safety in the digital environment. Without intending to go into the details of legal regimes, the paper emphasizes a kind of juxtaposition of the aspirations of modern society, that wants to achieve security through control and at the same time enable free development of children into adults.

Keywords: children, digital environment, internet, safety, culture of control

Introductory remarks – children in digital society

It can be said that modern society is a society of countless illuminated screens. These screens are not just a two-dimensional representation of traditional media content, on the contrary - they are the means by which the greatest interconnection of people and content is achieved. Digitalization have brought

* j.stojsic.dabetic@pravni-fakultet.info

unprecedented changes, and not only in the technological sense. The digital revolution has reached all segments of society, and changed the way human beings function even on a daily basis, from socialization to business, encompassing most things in between (Бјелајац и Филиповић 2021). The attribute that is most often attributed to modern society is digital, which is a consequence of the role and importance of digital technology, ie. information and communication technologies in everyday life. Modern society relies on digital technology, digital technology changes the basic paradigms of society, there are no activities or social factors that, to a greater or lesser extent, do not rely on different types of digital technology and modalities of its use. Children, in the sense of natural persons under the age of 18, as defined by the United Nations Convention on the Rights of the Child, are more than active users of digital technology. Having in mind the special responsibility that every society and legal system has in terms of ensuring the best interests of the child, and the status of children as a particularly vulnerable social group, and in the broader context of creating and developing a digital society, many legal, social, economic, security, moral and value issues related to the position of children, especially the position of children as users of digital technology.

Terminologically, the term child means a person under 18 years of age, and digital environment means information and communication technologies, in terms of technical means of transmitting information and through which it communicates (computer, hardware, software in the form of mobile phones, tablets, digital cameras and all other "smart" devices), including the Internet and digital media. The context of this paper is precisely the position of children in the digital environment, with special emphasis on the risks to the safety of children that occur in this context. New mobile and internet technologies create new opportunities for children's development, but at the same time create new risks. This creates a framework in which the socio-technological context influences the creation of security policy, but also vice versa (Stepanovic 2014, 169). For example, since the 1990s, the European Union has organized various initiatives and programs to achieve the safety of children in the digital society, such as the European Commission's Safer Internet Programs, the European Network of Safer Internet Centers, and European cybercrime prevention policy.

When it comes to the attitude of children towards the use of the Internet or. other types of digital communications, it is pointed out that children today live in the so-called. "interreality" as a new form of hybrid reality, which is a mixture of virtual and physical reality. Interactions between children today take place both on a virtual (online) and physical (offline) level, through various media used for communication (Kokswijk 2007, 40). Information and communication technologies are an important instrument in children's lives used for learning, socialization, expression, inclusion and enjoyment of children's rights and freedoms, but at the same time they are prone to endangerment of children's safety and instruments of potential violence against children. Using the Internet is a way for chil-

dren to fill the time between daily activities, and more and more daily activities have been moved to the online domain (e.g. watching television and even attending school). Today, it is quite common for children to use smartphones for everyday internet access, rather than any other means of digital communication, the data show that 57% of children use their phones in this way every day (children aged 9-11). In addition, children today can watch videos online, visit social networks (data show that 10% of children visit social networks daily in Germany and as many as 45% of children daily in Serbia), play online games and also use phones for school work. (Smahel et.al, 2020, 25). The data show that children mostly use the Internet for communication and entertainment, and less for other purposes. Also, in most European countries, children aged 14-16 spend twice as much time online as children aged 9-11 (Smahel et.al, 2020, 19). The level of digital skills of children is a basic precondition for successful use of the Internet, but with more usage, skills also grow, and with the growth of skills, following risks also increase.

The Council of Europe views the rights of the child in the digital environment as one of its priorities, which means creating an Internet that is safe, secure, open and accessible to all without discrimination. Also, children's rights, guaranteed by the UN Convention on the Rights of the Child, and the European Convention for the Protection of Human Rights and Fundamental Freedoms, must be and remain protected regardless of technological development. The UN Committee on the Rights of the Child proclaims that all children must have safe access to digital technology and digital communications, and be empowered to fully participate, express themselves, seek information and enjoy all the rights guaranteed by the children's human rights corpus. At the same time, the safety of children in online communications is regular subject of legal regulation nowadays, public policies and public debates - from criminal to educational, including the context of human rights and the rights of the child. The usefulness of the use of the Internet by children cannot be denied, but the growing and dangerous risks that arise from it cannot be denied, so the key question is how to protect children without restricting them too much in free development? And it is not disputable that the use of the Internet puts children in the position of potential victims, but also in the position of potential perpetrators of harmful behavior. Negative experiences that children had reported and encountered when using the Internet and other digital communications are, among other things, exposure to sexual content, aggressive content and other forms of unwanted content, then indecent contact, online abuse, sharing personal information, reputational damage, receiving viruses and online advertising (Cortesi and Gasser 2017, 22-24).

When question arises as to who is responsible for the safety of children in online communications, the most common answers are parents, then teachers in terms of achieving digital literacy in modern conditions of development of digital technologies and modalities of communication, as well as other social factors - NGOs, bodies that deal with the protection of children, as well as economic

entities, which bear part of the responsibility both directly in relations with children as users, and indirectly as support to parents and teachers. In online communication, it is very difficult for parents to notice the harmful contact that their child is exposed to. Parental supervision should be extended to their children's online communications, which include different modalities of Internet use, in the form of social networks, online games, virtual reality, forums, messaging, web use of webcams, etc., in different places - from school to streets all the way to the house, ie. wherever the phone is with them. And very often parents have very little insight into what is happening in the online world of their children, so they cannot even notice the risks and react in time. The memorandum to the Lanzarote Convention states the worrying phenomenon that children appear as victims of sexual assaults in online meetings, ie. interaction with adults that take place in cyberspace - internet chat rooms and game sites. The widespread availability of telephones makes this type of illicit behavior accessible to much younger children than adolescents, and thus makes the need for control mechanisms greater.

Experimental behavior, as well as behavior that involves certain risks, is, as experts agree, an integral part of growing up and emotional development of children, as well as creating their own identity, and all this happens through social contact, where today the Internet is positioned as a basic virtual space. creating and maintaining social contacts. On the other hand, the reality is that everything that is undertaken online is available to everyone and everywhere, practically globally, and any content can be, and is available to any search and duplication. It is often very difficult, almost impossible, to completely remove content posted on the Internet, just as it is quite easy to create fake profiles and place different content.

Legal framework of children's rights in digital society – child as active subject of digital environment

When a social aspect is imposed as a topic that has a significant impact on children, ie. where children are an important subject of social relations, the narrative is expected to set framework guidelines concerning the rights of the child as a special corpus of general human rights. The general framework of the rights of the child in the digital environment consists of fairly uniform settings within the system of the Council of the European Union and the European Union, which will be presented in a general way within this section.

Children "go online" even at the age of 4, and before going to school, they almost mastered surfing the net. For several hours a day, children are confronted with a world without any restrictions, so different from the world in which they normally live. So naive and innocent they easily become prey to internet predators. Predators have gained fast and anonymous access to

children via the Internet, a place where they can hide their identity and roam the web without restrictions. Internet predators are, in principle, sexual predators. We usually imagine them as people wandering around school playgrounds and stalking their potential victims there. However, the reality has changed. Today's sexual predators lurk for victims by hiding behind a computer screen, taking advantage of the excessive curiosity and gullibility of children and the anonymity offered by the Internet (Бјелајац и Филиповић 2020). Every child must be enabled to enjoy their rights and freedoms in the digital environment, ie. online and offline, specially right to life and right to development. States must introduce into their public policies regulation of the way in which society uses digital media, which has, or may have, consequences for the welfare of children. The basic principles on which the system of protection and enjoyment of children's rights in the digital environment is based include, among other things, the realization of the best interests of the child, the prohibition of discrimination, the child's right to be heard, respect for the individual abilities of the child, the primary responsibility of the state to ensure respect and enjoyment of children's rights in the digital environment, the right to free access and use of digital technology, the right to freedom of expression and information, the right to participate, the right to play and association, the right to privacy and data protection, digital literacy, and the right to protection and security (Ad hoc Committee for the Rights of the Child (CAHENF)).

Achieving the best interests of the child means that the protection of the child is achieved in balance with the right to freedom of expression and with the participation of the child in deciding on issues that concern him. The prohibition of discrimination does not prevent the adoption of special measures aimed at children who belong to vulnerable groups, bearing in mind that the digital environment can deepen this vulnerability, but at the same time it can eliminate it. In the digital environment, children must be able to participate in decision-making, in accordance with their abilities according to age and maturity, as well as to express themselves freely using different media, while at the same time ensuring the effective participation of children in the development, implementation and evaluation of policies, mechanisms, practices, technologies and resources aimed at promoting, protecting and enjoying their rights in the digital environment. The state and other actors must take into account the abilities of children, bearing in mind children with special needs, disabilities, and ensure that the policies adopted correspond to their needs and the development of their potential in the digital environment.

Restricted or completely denied access to the digital environment deprives children of the full enjoyment of their guaranteed rights. States have an obligation to provide access to devices, connectivity and content in a secure and accessible manner. Particular attention must be paid to vulnerable groups of children, such as children in foster care, children deprived of their liberty or children

whose parents are deprived of their liberty, migrant children and children in rural areas. States must influence providers to ensure that their services are accessible to children in an appropriate manner, especially from the point of view of child safety as a user and content appropriate to children as users. States must respect the role of children as creators and transmitters of information. their responsibilities in that regard, especially in relation to the rights of others. The digital environment enables gathering and association through online communication and participation, ie. creating and maintaining social contacts via the digital network, as well as appropriate ways for children to express themselves and be creative, while respecting their copyrights. In these activities, children must be given an insight into their rights and ways of protection, in an appropriate way. States must protect the privacy of children, personal information, online reputation and the confidentiality of correspondence, both in relation to the state itself and in relation to other factors. The processing of data relating to children must be lawful and fair, secure, with the clear consent of the data subject, in accordance with legal guarantees. Special attention must be paid to the principles of privacy by design and the principle of privacy by default. Privacy and data processing notices must be such that children can understand them and give their informed consent accordingly. Digital literacy must be part of the earliest primary education curriculum, and implies the development of competencies for the use of digital technology, as well as the skills of content creation and critical understanding of the digital environment. Children must be protected from risks to their physical and mental health, especially in relation to sexual exploitation and abuse. The safety of children should be achieved so that other rights, especially those aimed at the development of children, are not too restricted. States must ensure the promotion of the principle of safety design as a guiding principle in the production of devices and services aimed at children as users, as well as introduce age verification systems when using devices and services. Security includes the prevention of serious crimes that take place in cyberspace, as well as the prevention of the placement of illegal or harmful content and materials, including material that constitutes child abuse.

Children as subjects of legal framework for the protection of privacy

General data protection regulation of the European Union on the protection of personal data refers specifically to the protection of children and personal data in the digital world. Recital 38 especially emphasizes that children, as a special category of users of digital technology, are less aware of the risks, consequences and security measures, as well as their rights within the process of personal data processing. The aim of the protection system provided by the Regulation is special protection against re(use) of children's personal data for the needs of marketing and other commercial services. In practice, children are often unable to understand the nature of the data processing process, in terms of what

data is processed, how it is processed and who the processor is. Furthermore, they are not always able to understand the consequences of the data processing process, as well as to understand their legal position in the data processing process, and thus to use their rights effectively.

Article 8 of the Regulation defines distribution of powers regarding decisions on lawful processing of personal data on children into the hands of parents or legal guardians, in cases where children are unable to understand and are not sufficiently aware to be able to make independent decisions. According to Regulation, for children under the age of 16 whose data are being processed the consent of the parents is required. States may set a lower age limit, but not less than 13 years of age.

If the parental consent, or consent of child set as the primary line of defense for child safety in the digital society, then all the weaknesses of the legal concept of consent also apply to the condition of parental consent for the processing of data about the child. Namely, consent implies that by giving consent we establish control over the processing of our personal data, ie. that we have a real choice and understand the practice of data processing by the processor. Legally speaking, the entity participating in the consent transaction by giving consent, ie. the consenting party must have a sufficient level of judgment and sufficient information, in particular on the consequences of giving consent. This makes children and people with mental disorders incapable of giving informed consent as a legally valid consent (Custers et.al, 2013, 438). In practice, if we want to sign up for online services or use applications, the only option is to agree to the privacy policy that is a prerequisite for use. The only options offered to the user on this occasion are "I accept" or "I do not accept". Furthermore, very often users do not read privacy policies at all, or read them but do not understand them, and there are not a small number of applications in which the privacy policy is not highlighted at all (Schermer and Custers and Van der Hof 2014, 6).

Children under the age of 13 must have parental consent to use the services, even when those services, services or applications are free. And parental consent must be verifiable. Verifiability of parental consent implies that reasonable efforts must be made by the service provider or data processors to ensure that it is indeed the parent who has given consent, and no particularly reliable mechanisms for such verification have been established at the level of practice yet.

In practice, giving a child the opportunity to give consent is problematic on several levels, but on the other hand, insisting on parental consent leads to the creation of tension between children and parents regarding the expectation of respect for privacy. Social networks, in addition to being forum for communication with peers, provide a space in which young people expect a certain degree of privacy, outside of parental supervision, and strict insistence on parental consent can lead to parental supervision that is unacceptable. Request for parental

consent in the case of children under 13 or 16 years can negatively affect the rights of emancipation and participation rights of these children and the creation of their digital environment, lead to a higher level of parental control and thus endanger the rights of children's privacy, especially in adolescents for whom online private space is as important as non-virtual one (free of parental supervision). Some online services may be disabled by this conditions. Achieving security in the processing of children's personal data may jeopardize other rights and freedoms of children.

In addition to parental consent, the Regulation provides for several other, general, mechanisms that can contribute to child safety, although they are not designed specifically for child protection - the principles of privacy by design and privacy by default as well as data processing impact assessment. In the context of child protection, they imply the obligation of controllers and data processors to take into account the realization of the best interests of the child when creating their operational, technical and organizational processes. The principles of privacy by design and privacy by default imply that controllers implement data protection principles in their data processing systems. Privacy by design means that the controller applies appropriate technical and organizational measures (like pseudonymization) that are created precisely as an expression of the principles of data protection, as well as that the data processing process itself is in accordance with the principles of data protection. The principle of privacy by default implies that controllers apply appropriate technical and organizational measures that ensure that only personal data that are necessary for the specific processing in question are processed. These two principles are, in practice, more related to technological design, rather than to organizational measures, in terms of internal policy and practice (Van der Hof and Lievens 2017, 3-7). Given the high degree of vulnerability of children as a social group and users of digital technology, special treatment of the application of the principle of privacy by design and the principle of privacy by default is justified when it comes to systems in which children's data is processed, such as educational and administrative systems and care systems.

Furthermore, the Regulation explicitly emphasizes the need to protect children in relation to the transparency of data processing practices, which in practice means that data processing process must be created in accordance with children's perception, experience and expectations, and especially adapted to different ages of children that access such content, while keeping in mind the degree of understanding that children can have about the digital economy and the digital environment in general. Also, it is recommended that profiling, as a result of data processing, should not be applied if the data indicate that the user is a child or a person under 18 years of age. Regarding the right to be forgotten, upon reaching the age of majority, the subjects who processed the data of the person who was a minor at that time, must obtain a new consent for further data processing or, in case of denial of consent, remove that data.

The Regulation also stipulates the obligation for the controller to assess the impact of data processing processes that may result in a high risk to the rights and freedoms of the persons whose data are processed, before the data processing itself. Since children are considered a particularly vulnerable group, this indicates the need to conduct an assessment whenever it comes to children's data.

In the case of video surveillance in schools, and related to guarantees of protection of personal rights, the school is the controller of data collected, held, processed and used, and can only collect data to which the law or the consent of the person whose data it collects authorized (by law or by personal authorization) for the prescribed purpose, in accordance with the principles of data accuracy, expediency of processing and proportionality of processing. Thus, the processing of student personal data falls within the general framework of personal data protection.

In schools, children, as students, can be subject to data processing through video surveillance of public space, which includes the space in front of the school, entrance to the school or access to official premises, corridors, in order to achieve student safety. Areas where users expect a higher degree of privacy are excluded from the subject of video surveillance - toilets, locker rooms, rest areas, etc. In the practice of expert bodies for the protection of personal data, video surveillance is considered to be the last tool used in exceptional cases, when the purpose of security cannot be achieved by milder means. In essence, the subject of video surveillance must be areas where security must be protected, but security can, and often is, more endangered within areas that are excluded from video surveillance coverage, of which schools are no exception.

The purpose of processing data on students, in the context of video surveillance in schools, is security, but care must be taken in all ways, less invasive ways, and in accordance with the guarantees of the right to privacy and human dignity, this purpose can be achieved during the stay children in school, especially within the premises where both students and teaching staff (Commissioner for Information of Public Importance and Personal Data Protection (ПИЈЗПЛ) 2019, 33-34).

Children and young people in their activities cannot avoid the trend of supervision in modern society. When it comes to supervision, there are two sides: control and care. Surveillance may identify unacceptable, harmful or even illegal behavior, but can also contribute to the protection of the individual. Any form of supervision must be created to enable the individual its personal development.

The culture of control as a narrative in the context of the use of digital technology by children

During adolescence, children should reach a certain degree of independence and a sense of personal freedom, both in their relationships and in their

relationships with their parents, which takes place through a process of independent decision-making and self-reliance, with the continuing need for parental support. Parental control during adolescence should also be less extensive.

The safety of children, whether it is the use of digital technology or other contexts, is primarily the responsibility of parents or guardians, but when they are not able to do so or when risks exceed their capabilities, public policies must provide protection to children. When it comes to child safety, as in any other context of public policies relating to children and youth, an important goal is to achieve and respect the self-development and freedom of children as individuals (Cortesi and Gasser 2017, 100-102). Personal autonomy during childhood and adolescent development contributes to growing into responsible and independent adult individuals, and it is necessary during the period of development to engage in experimental behavior, engage in various risks and research. Behaviors that pose too great a risk must certainly be disabled or controlled, but at the same time a sufficient degree of freedom must be left to achieve the developmental goals of each child (Van der Hoff, Koops 2011, 3-4).

Independent establishment and maintenance of social relations, in the real world and online, is a process of mistakes and learning through which the independence of a person is acquired. In all of this, especially in the realm of digital communications, young people often feel invincible and untouchable, and are often unaware of the risks their behavior carries with. They also have less ability to assess the seriousness of the risks they take, as well as lack of awareness of the consequences that their behavior can cause, both for them and for their immediate environment. High parental involvement in children's ways of using the Internet leads to a greater degree of security, but limits the experience of using the Internet and developing digital skills and gaining experience in avoiding harmful behaviors. What needs to be achieved is an open dialogue between parents and children, which results in an understanding of online experiences, skills and respect for the rights of others. (Cortesi and Gasser 2017, 26-29) .

Public policies related to the use of the Internet by minors are necessary in modern society, as an additional mechanism for parental supervision in terms of achieving the safety of children. These policies lie between two extremes: a culture of control based on risk management and fostering children's autonomy that develops precisely through risk-taking. This conditions the content of policies in the direction of raising awareness, stimulating self-control, technological measures, responsibility, criminalization and legal regulation. Fear of what may happen to children, bearing in mind that policy makers are often people who are themselves parents, naturally conditions the content of policies towards increasing control over the behavior of young people - from the family level, through school and all to public policies.

The establishment of mechanisms that enable control is today a social trend, which affects the perception of hitherto socially acceptable behaviors as potentially dangerous or introduction to crime (for example offering a ride to a

young person is today considered unacceptable behavior that young people should avoid), schools are seen as a kind of fortress, and students as a population of potential victims or offenders. The trend has been adopted that as many youth activities as possible should be supervised. Public policies related to digital security balance between freedom and control of the use of the Internet by children, while cybercrime prevention policies often focus unilaterally on control, with an emphasis on criminal protection, while neglecting the importance of learning through personality development errors (Van der Hoff, Koops 2011, 10). The one-sidedness of criminal protection can ultimately result in inefficiency, even counterproductivity in relation to the response of children to be protected. In digital communication, young people find both risks and opportunities.

By embracing a culture of control, civil society is becoming less tolerant of independence and less willing to trust, and this creates a modern childhood framework for today's generations. The culture of control relies heavily on criminal law and the severity of the penalties provided. Public policies in this domain are created within the framework of risk or risk identification, assessment and control, combined with the need to avoid risk in order to create a "safe state" in which the absence of actual or perceived danger is the highest value that takes precedence over all other objectives.

Conclusion

Today, children are active actors in the digital environment, at the same time positioned as subjects of public policies aimed at achieving the safety of children in the digital environment. Today, the Internet is an unavoidable element in growing up, and that implies a sufficient degree of media or digital literacy or abilities as a parent or guardians as well as children. It is very questionable how many children, as consumers of digital technology, can understand their personal and wider digital environment. Achieving a high level of digital literacy and awareness of the need and ways of safe behavior on the Internet should be the backbone of public child safety policies in the digital society. Also, parents need to be aware of the risks that exist for interactions in the digital environment, so that they can spot and respond to them in a timely manner. Basing public policies on the culture of control as a narrative in the context of the use of digital technology by children, indicates the creation of a new paradigm of childhood. The modern concept of childhood today is based on the need to strike a balance between the freedom of children to develop into responsible and independent adults and the need to control the risks that exist in digital communication and the digital environment.

References

1. Бјелајац, Жељко Ђ. и Александар М. Филиповић. 2020. „Интернет и друштвене мреже као неограничени простор за концентрацију и мултиплицирано присуство педофила". У: „Педофилија – узроци и последице", ур. Жељко Ђ. Бјелајац и Александар М. Филиповић, посебно издање, *Култура полиса,* 29-40
2. Бјелајац, Жељко Ђ. и Александар М. Филиповић. 2021. „Флексибилност дигиталних медија за манипулативно деловање сексуалних предатора". *Култура полиса,* XVIII (44): 51-67, https://doi.org/10.51738/Kpolisa2021.18.1r.2.01.
3. Ad hoc Committee for the Rights of the Child (CAHENF), Drafting Group of Specialists on Children and the Digital Environment (CAHENF-IT). 2017. *Recommendation CM/REC(2018)x of the Committee of Ministers to Member States on Guidelines to promote, protect and fulfil children's rights in the digital environment*, Strasbourg.
4. Cortesi, S. and Gasser, U. (Eds.). 2015. Digitally connected: Global perspectives on youth and digital media, Berkman Center Research Publication No. 2015-6.
5. Custers, Bart and van der Hof, Simone and Schermer, Bart and Appleby-Arnold, Sandra and Brockdorff, Noellie. 2013. "Informed Consent in Social Media Use – The Gap between User Expectations and EU Personal Data Protection Law" *Script-ed: A Journal of Law and Technology* 10(4), 435-457.
6. Повереник за информације од јавног значаја и заштиту података о личности (ПИЈЗЗПЛ). 2019. *Заштита података о личности: ставови и мишљења Повереника*, Публикација бр. 4, Београд.
7. Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), Official Journal of the European Union, 2016/L119
8. Schermer, Bart and Custers, Bart and Van der Hof, Simone. 2014. „The Crisis of Consent: How Stronger Legal Protection may lead to Weaker Consent in Data Protection" *Ethics and Information Technology*, DOI: 10.1007/s10676-014-9343-8.
9. Smahel, D., Machackova, H., Mascheroni, G., Dedkova, L., Staksrud, E., Ólafsson, K., Livingstone, S., and Hasebrink, U. 2020. *EU Kids Online 2020: Survey results from 19 countries*, EU Kids Online. Doi: 10.21953/lse.47fdeqj01ofo.
10. Stepanovic, Ivana. 2014. „Modern technology and challenges to protection of the right to privacy" *Annals FLB – Belgrade Law Review*, Year LXII, No. 3, 167-178.

11. Van der Hof, Simone and Koops, Bert-Jaap. 2011. „Adolescents and Cybercrime: Navigating between Freedom and Control" *Policy & Internet*, Vol. 3, Iss. 2, Art. 4.
12. Van der Hof, Simone and Lievens, Eva. 2017. „The importance of privacy by design and data protection impact assessments in strengthening protection of children's personal data under the GDPR" Presented at the IALS Conference *Children and Digital Rights: Regulating Freedoms and Safeguards* (17 October 2017, London), To be published in: Communications Law 2018, Vol. 23, No. 1.
13. Van Kokswijk, J. 2007. *Digital Ego: Social and Legal Aspects of Virtual Identity*, Delft: Eburon Uitgeverij, ISBN-13: 978-9059722163 (navedeno prema Van der Hof, Simone and Koops, Bert-Jaap. 2011. „Adolescents and Cybercrime: Navigating between Freedom and Control" *Policy & Internet*, Vol. 3, Iss. 2, Art. 4).